

REPORT DOCUMENTATION PAGE			Form Approved OMB NO. 0704-0188		
<p>The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA, 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</p> <p>PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.</p>					
1. REPORT DATE (DD-MM-YYYY) 07-12-2016		2. REPORT TYPE Final Report		3. DATES COVERED (From - To) 11-Aug-2014 - 10-Aug-2016	
4. TITLE AND SUBTITLE Final Report: Cognitive Medical Wireless Testbed System (COMWITS)			5a. CONTRACT NUMBER W911NF-14-1-0554		
			5b. GRANT NUMBER		
			5c. PROGRAM ELEMENT NUMBER 611103		
6. AUTHORS Vuk Marojevic, Deven Chheda, Raghunandan Rao, Randall Nealy, and Jeffrey H. Reed			5d. PROJECT NUMBER		
			5e. TASK NUMBER		
			5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAMES AND ADDRESSES Virginia Polytechnic Institute & State Univ North End Center, Suite 4200 300 Turner Street, NW Blacksburg, VA 24061 -0001			8. PERFORMING ORGANIZATION REPORT NUMBER		
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES) U.S. Army Research Office P.O. Box 12211 Research Triangle Park, NC 27709-2211			10. SPONSOR/MONITOR'S ACRONYM(S) ARO		
			11. SPONSOR/MONITOR'S REPORT NUMBER(S) 65180-NS-RIP.6		
12. DISTRIBUTION AVAILABILITY STATEMENT Approved for Public Release; Distribution Unlimited					
13. SUPPLEMENTARY NOTES The views, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy or decision, unless so designated by other documentation.					
14. ABSTRACT Future mobile broadband systems will need to be of high availability and flexibility to support mission-critical applications and new spectrum management paradigms. Testbeds shall play a major role in developing and testing these new wireless communications technologies and systems. Over the years, Wireless@Virginia Tech has built testbeds that enable research and education on dynamic spectrum access and 4G LTE, among others, using software-defined radio (SDR) technology. The 48-node Cognitive Radio					
15. SUBJECT TERMS Amarisoft, CMW500, COMWITS, GNU Radio, LTE, RFNEST, srsLTE, SDR, USRP, MIMO, CORNET, UE simulator					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON Jeffrey Reed
a. REPORT UU	b. ABSTRACT UU	c. THIS PAGE UU			19b. TELEPHONE NUMBER 540-231-2972

Report Title

Final Report: Cognitive Medical Wireless Testbed System (COMWITS)

ABSTRACT

Future mobile broadband systems will need to be of high availability and flexibility to support mission-critical applications and new spectrum management paradigms. Testbeds shall play a major role in developing and testing these new wireless communications technologies and systems.

Over the years, Wireless@Virginia Tech has built testbeds that enable research and education on dynamic spectrum access and 4G LTE, among others, using software-defined radio (SDR) technology. The 48-node COgnitive Radio Network (CORNET) testbed spans the 4 floors of a campus building, whereas 12 outdoor nodes of O-CORNET are deployed on rooftops across campus for outdoor experiments. The LTE-CORNET testbed located at 475 Durham Hall allows for testing and evaluation of LTE systems for education and research. All testbed nodes are remotely accessible by registered users.

Instead of having another dedicated testbed for supporting COMWITS (Cognitive Medical Wireless Testbed System) waveforms for medical applications, it is more effective if the capabilities of the existing testbed architecture are extended, and reutilized. The new combined testbed would then allow testing of various waveforms on common hardware through the use of existing and new USRPs, emulators, antennas and test equipment. Non-radiating and over-the-air modes will be possible by switching between channel emulators and antennas.

Enter List of papers submitted or published that acknowledge ARO support from the start of the project to the date of this printing. List the papers, including journal references, in the following categories:

(a) Papers published in peer-reviewed journals (N/A for none)

<u>Received</u>	<u>Paper</u>
-----------------	--------------

TOTAL:

Number of Papers published in peer-reviewed journals:

(b) Papers published in non-peer-reviewed journals (N/A for none)

<u>Received</u>	<u>Paper</u>
-----------------	--------------

TOTAL:

Number of Papers published in non peer-reviewed journals:

(c) Presentations

Vuk Marojevic, "Virginia Tech's Cognitive Radio Network (CORNET) Testbeds", White Paper and Presentations, Large-scale Networking Platforms "Communities of Practice" Workshop, Arlington, VA, Oct. 24-25, 2016, <http://www.winlab.rutgers.edu/events/tbcopws/WP.html>

Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

<u>Received</u>	<u>Paper</u>
12/05/2016	3.00 Mina Labib, Vuk Marojevic, Jeffrey H. Reed, and Amir I. Zaghloul. How to enhance the immunity of LTE systems against RF spoofing, 2016 International Conference on Computing, Networking and Communications (ICNC). 15-FEB-16, Kauai, HI, USA. : ,
12/05/2016	1.00 Mina Labib, Vuk Marojevic, Jeffrey H. Reed. Analyzing and enhancing the resilience of LTE/LTE-A systems to RF spoofing, 2015 IEEE Conference on Standards for Communications and Networking (CSCN). 28-OCT-15, Tokyo, Japan. : ,
TOTAL:	2

Number of Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Peer-Reviewed Conference Proceeding publications (other than abstracts):

<u>Received</u>	<u>Paper</u>
TOTAL:	

Number of Peer-Reviewed Conference Proceeding publications (other than abstracts):

(d) Manuscripts

<u>Received</u>	<u>Paper</u>
TOTAL:	

Number of Manuscripts:

Books

Received Book

TOTAL:

Received Book Chapter

TOTAL:

Patents Submitted

Patents Awarded

Awards

Graduate Students

NAME	PERCENT SUPPORTED	Discipline
Raghunandan R. Rao	0.00	
Deven Chheda	0.00	
Mina Labib	0.00	
Durga Laxmi Narayana Swamy Int	0.00	
Kevin Ryland	0.00	
Sai Nisanth Bodepudi	0.00	
FTE Equivalent:	0.00	
Total Number:	6	

Names of Post Doctorates

<u>NAME</u>	<u>PERCENT SUPPORTED</u>
-------------	--------------------------

FTE Equivalent:

Total Number:

Names of Faculty Supported

<u>NAME</u>	<u>PERCENT SUPPORTED</u>	National Academy Member
Jeffrey H. Reed	0.00	
Taeyoung Yang	0.00	
Vuk Marojevic	0.00	
FTE Equivalent:	0.00	
Total Number:	3	

Names of Under Graduate students supported

<u>NAME</u>	<u>PERCENT SUPPORTED</u>
-------------	--------------------------

FTE Equivalent:

Total Number:

Student Metrics

This section only applies to graduating undergraduates supported by this agreement in this reporting period

The number of undergraduates funded by this agreement who graduated during this period: 0.00

The number of undergraduates funded by this agreement who graduated during this period with a degree in science, mathematics, engineering, or technology fields:..... 0.00

The number of undergraduates funded by your agreement who graduated during this period and will continue to pursue a graduate or Ph.D. degree in science, mathematics, engineering, or technology fields:..... 0.00

Number of graduating undergraduates who achieved a 3.5 GPA to 4.0 (4.0 max scale):..... 0.00

Number of graduating undergraduates funded by a DoD funded Center of Excellence grant for Education, Research and Engineering:..... 0.00

The number of undergraduates funded by your agreement who graduated during this period and intend to work for the Department of Defense 0.00

The number of undergraduates funded by your agreement who graduated during this period and will receive scholarships or fellowships for further studies in science, mathematics, engineering or technology fields:..... 0.00

Names of Personnel receiving masters degrees

<u>NAME</u>
Raghunandan M. Rao
Deven Chheda (MEng)

Total Number: 2

Names of personnel receiving PHDs

<u>NAME</u>

Total Number:

Names of other research staff

<u>NAME</u>	<u>PERCENT SUPPORTED</u>
Randall Nealy	0.35
FTE Equivalent:	0.35
Total Number:	1

Sub Contractors (DD882)

Inventions (DD882)

Scientific Progress

This testbed merges two ARO grants: #W911NF-14-1-0553 and #W911NF-14-1-0554. See detailed project report.

Technology Transfer



Cognitive Medical Wireless Testbed System (COMWITS)

System Overview and Performance Report

Vuk Marojevic, Deven Chheda, Raghunandan Rao, Randall Nealy, and Jeffrey H. Reed

Document Control and Data Sheet

Document No.	1
Document Title	Cognitive Medical Wireless Testbed System (COMWITS): System Overview and Performance Report
Date	November 2016
Type of document	Technical
No. of pages	88
Authors	Vuk Marojevic, Deven Chheda, Raghunandan M. Rao, Randall Nealy, and Jeffrey H. Reed
Abstract	This document presents an overview of the COMWITS system and its components. The hardware and software aspects are described first, followed by networking and user access management. A user manual is included for quick access to the most used functions. Measured results from the initial studies carried out for the proof-of-concept for 2x2 MIMO are presented and compared against expected values from 3GPP specifications.
Keywords	Amarisoft, CMW500, COMWITS, GNU Radio, LTE, RFNEST, srsLTE, USRP, MIMO, CORNET, UE simulator
Project	COMWITS
Project Award	Army Research Office DURIP grant W911NF-14-1-0554

Table of Contents

Abbreviations	4
List of Figures	5
List of Tables	7
1 Introduction	8
2 System Overview	10
3 Hardware	13
3.1 CMW500	13
3.2 Computing Nodes	13
3.3 Software Radio Peripherals	15
3.4 RF Processing	17
3.5 Channel Emulator	17
3.6 RF Filters	18
3.7 Antenna system	19
3.8 User Equipment	19
3.9 Spectrum Analyzer	20
3.10 Reference Oscillator and Clock Source	20
3.11 RF Switches	21
4 Software	22
4.1 Wireless Communications Software	23
4.2 Performance Analysis Software	24
5 Networking and User Access	25
6 User Manual	27
6.1 User Registration and General Usage Instructions	27

6.2	Accessing the Testbed	27
6.3	Configuring the Testbed	32
7	System Administration	41
8	Testbed Use in Research and Education	42
8.1	Education	42
8.2	Research	43
9	Conclusions and Lessons Learned	45
	References	47
 <u>Appendix</u>		
A	Modulation and Coding Schemes in LTE	49
B	Theoretical LTE Peak Throughput	51
C	Transmission Modes in LTE	56
D	UE Categories in LTE	58
E	Initial Measurements for 2x2 LTE-MIMO: Cabled Mode	59
F	Initial Measurements for 2x2 LTE-MIMO: Over-the-Air Mode	65
G	Initial Measurements for 2x2 LTE-MIMO: Channel Emulation Mode	70
H	RFnest Attenuation Data	73
I	Software Development for the Testbed	75
J	CMW500 License Keys	77
K	FCC Experimental License Application Process	78
L	FCC Emissions Table	81
M	Equipment List	84
N	Scholarly Research Contributions	88

Abbreviations

CEC	Channel Emulator Controller
COMWITS	Cognitive Medical Wireless Testbed System
CORNET	Cognitive Radio Network
CP	Cyclic Prefix
CQI	Channel Quality Indicator
DL	Downlink
FDD	Frequency Division Duplex
GRC	GNU Radio Companion
LTE	Long Term Evolution
MCS	Modulation and Coding Scheme
MIMO	Multiple-Input Multiple-Output
O-CORNET	Outdoor CORNET
OTS	Off-the-Shelf
PDSCH	Physical Downlink Shared Channel
PUSCH	Physical Uplink Shared Channel
PRB	Physical Resource Block
QAM	Quadrature Amplitude Modulation
QoS	Quality-of-Service
QPSK	Quadrature Phase Shift Keying
RB	Resource Block
RE	Resource Element
Rfnet	Radio Frequency Network channel Emulation Simulation Tool
RI	Rank Indication
RSRP	Reference Signal Received Power
RSRQ	Reference Signal Received Quality
SDR	Software-Defined Radio
SISO	Single Input Single Output
TBS	Transport Block Size
TDD	Time Division Duplex
TTI	Transmission Time Interval
UDP	User Datagram Protocol
UE	User Equipment
UHD	USRP Hardware Driver
UL	Uplink
USRP	Universal Software Radio Peripheral

List of Figures

Figure 1. LTE-CORNET/COMWITS testbed - main system components.

Figure 2. Functional RF diagram for all testbed operational modes including 2x2 MIMO.

Figure 3. Photo of CMW500.

Figure 4. Mobile node with B210 USRP.

Figure 5. Computing node with four B210 USRPs.

Figure 6. RFnest hardware showing the 8 RF ports and Ethernet interface.

Figure 7. Omni-directional, ceiling mounted antenna [3].

Figure 8. UEs.

Figure 9. RF Spectra of two adjacent 10 MHz LTE cells. The left band shows a TD-LTE signal spectrum, generated by the Amarisoft LTE100 eNB with N210 USRP. The power level histogram shows peaks at -95 and around -117 dBm because of the different received power levels of the UL and DL signals. We also see the SDR's local oscillator leakage at the carrier frequency at 2680 MHz. The right band shows a clean FD-LTE downlink signal spectrum, generated by the CMW500, with full resource allocation.

Figure 10. Internal network layout.

Figure 11: Example SSH (putty) login screen and command prompt.

Figure 12: Example command screen showing port number displayed after running `$ x11vnc`

Figure 13: Sample TightVNC Viewer screen.

Figure 14a-d: Ensuring OpenVPN software has administrator privileges.

Figure 15a,b: Connecting using OpenVPN.

Figure 16a,b: Launching PuTTY.

Figure 17a,b: Launching the remote desktop server.

Figure 18: Launching TightVNC Viewer.

Figure 19: Launching Remmina to connect to CMW500.

Figure 20: The CMW500 interface.

Figure 21: Launching CEC using the terminal.

Figure 22: Launching RFview script using the terminal.

Figure 23: RFview GUI showing a loaded scenario.

Figure 24: Initializing the RFnest hardware using RFview GUI.

Figure 25: Confirmation message displayed after successful initialization of the RFnest hardware.

Figure 26: Performing a reset on the CMW500 prior to an experiment.

Figure 27: Turning the Signal Generator ON/OFF using the CMW500 interface.

Figure 28a,b: Configuring the Rogers UE.

Figure 29: JPerf (a GUI interface for iPerf) reporting throughput in real-time.

Figure 30: Constellation diagram of the four 16-QAM data streams of the FMT-FBMC waveform.

Figure 31: Snapshot showing the stages of forced handover with the forced handover feature of LTE100.

Figure. 32: Experiment setup for the LTE vulnerability analyses of [26] [27] [29].

List of Tables

Table 1. Testbed features.

Table 2a-c. Computer specifications (shaded columns indicate LTE-CORNET equipment).

Table 3. USRP Specifications (shaded columns indicate LTE-CORNET equipment).

Table 4. RFnest Specifications (bold frequencies are supported by our RFnest units).

Table 5. Filter bank assignments.

Table 6. Electrical parameters of the antenna [3].

Table 7. UE Specifications.

Table 8. RF Switch Settings.

Table 9a-c. Software installed on processing nodes (shaded columns indicate LTE-CORNET equipment).

Table 10. Networking specifications.

1. Introduction

Future mobile broadband systems will need to be of high availability and flexibility to support mission-critical applications and new spectrum management paradigms. Testbeds shall play a major role in developing and testing these new wireless communications technologies and systems.

Over the years, Wireless@Virginia Tech has built testbeds that enable research and education on dynamic spectrum access and 4G LTE, among others, using software-defined radio (SDR) technology. The 48-node COgnitive Radio Network (CORNET) testbed spans the 4 floors of a campus building, whereas 12 outdoor nodes of O-CORNET are deployed on rooftops across campus for outdoor experiments. The LTE-CORNET testbed located at 475 Durham Hall allows for testing and evaluation of LTE systems for education and research. All testbed nodes are remotely accessible by registered users.

CORNET is currently used for the student spectrum sharing radio contest (Spectrum-ShaRC), where student teams develop and test cognitive engines using the in-house developed cognitive radio test system software. It is also used for developing visualization and gamification tools (CORNET-3D) for undergraduate STEM education. The LTE-CORNET testbed is a unique facility for LTE education and research and features industry-grade/commercial and SDR LTE systems, open-source waveforms and channel emulators that support our experimental research on LTE for mission-critical communications. By combining a modular set of hardware and software components, the testbed has the following salient features:

- Remote access to a controlled experimental environment,
- Reproducible experimentation capability,
- Rapid setup of multiple emulated LTE cells (3GPP compliant, Releases 8-12), up to five cells simultaneously
- Real user equipment (UEs),
- Access to commercial and free open-source code,
- Over-the-air or nonradiating experiments, and
- Flexibly configurable and easily upgradeable.

Instead of having another dedicated testbed for supporting COMWITS (Cognitive Medical Wireless Testbed System) waveforms for medical applications, it is more effective if the capabilities of the existing testbed architecture are extended, and reutilized. The new combined testbed would thus then allow testing of various waveforms on common hardware through the use of existing and new USRPs, emulators, antennas and test equipment. Non-radiating and over-the-air modes will be possible by switching between channel emulators and antennas. Some of the upgrades include the addition of a second channel emulator for frequencies below 2 GHz, and a simplified channel emulator consisting of discrete RF components for additional signal generation capabilities. Thus, in addition to the salient features described earlier, the combined testbed additionally offers the following capabilities including:

- Support for additional radios and protocols,
- Generation of waveforms in controlled environments and evaluating them for use in both body area networks and in hospital environments,

- Capability for analyzing different types of wireless systems, including local area networks for gathering healthcare-related information from sensors,
- Versatility of creating different levels of harsh signaling and propagation environments to analyze the best protocols to use for transmitting real-time sensor data, and
- Comparison of waveforms of LTE and WiFi under identical channel conditions.

2. System Overview

The core of the COMWITS testbed is located in 475 Durham Hall (server room). Figure 1 shows a photo.

The testbed's main components are several LTE base stations (eNodeBs) with their evolved packet cores (EPCs), two channel modes, and several LTE user equipment (UEs). One eNodeBs is the Rohde & Schwarz CWM500, a industry standard eNodeB emulator and UE tester and the other is Amarisoft software-defined radio (SDR) LTE100 system installed on PCs and mobile workstations. A third open-source SDR library called srsLTE is available as well.

The RF signals can access the wireless channel through seven antenna ports. Five fixed antennas are deployed in the ceiling of Wireless@VT's RF laboratory. Alternatively, the signals can be routed through two configurable channel emulators called RFnest which operate at different frequency bands. RFnest's 8-port analog system A208, allows for non-radiating experiments in a controlled RF environment. Several UEs of different categories and types are available, including Cat. 4, 5 and 6 devices in the form of USB dongles, access points or smartphones. A shielded box can be used for over-the-air experiments. An FCC experimental license for several bands is available through O-CORNET [1] [28]. The testbed uses two eight port channel emulators called Radio Frequency Network Emulator Simulator (RFnest) and an attenuator bank. Table 1 summarizes the main features.



Figure 1. LTE-CORNET/COMWITS testbed - main system components.

The present design uses a switching network to select individual device ports for interfacing with other devices. For 2x2 MIMO operation, the transmitter and receiver both require two ports each to be selected simultaneously, which is equal to half the number of ports on the channel emulator. Apart from the USRPs and UEs, separate connections need to be provided to connect to the CMW500, to external antennas, and

to additional equipment in the RF lab. This would require choosing eight ports out of available thirteen ports such that the simultaneous requirement of the MIMO devices is satisfied.

One way of accomplishing this is through the use of a series of cascaded switches, or a RF switching matrix which is costly. To keep the cost low and to maximize the reuse of existing hardware, a new approach to the problem was considered where the device ports were ranked in terms of priority and several operational scenarios were considered. Using the assigned priority levels, combinations of these device ports were grouped to eliminate combinations of device ports that wouldn't be used at all. In the end, the selected combinations enabled switching between the 2x2 MIMO mode of operation and the earlier mode of operation with the addition of only one 8-switch bank to the present setup. Operating at 4x4 and higher modes would require additional ports on the network emulators, 4-port UEs and additional RF switching.

Figure 2 indicated the two main configurations of the testbed, the cabled mode using channel emulators and over-the-air mode using antennas. The RF paths are shown in green in Fig. 2. The three connections leaving the diagram on the right are connections to the RF lab to connect to other lab equipment.

Five fixed antennas are placed in the ceiling of the adjacent RF lab, in 471 Durham Hall. The aforementioned RF ports are available for connecting user-provided equipment to the testbed. All 8 are connected to the testbed through the conduit in the wall. All cables are 40 ft long.

The testbed is remotely accessible and configurable through the Internet.

Appendix M provides the complete equipment list and includes the components that were purchased for the LTE-CORNET testbed under ARO/DURIP grant #W911NF-14-1-0553.

Table 1. Testbed features.

Feature	Support
Standards	3GPP LTE Rel. 8-12 ¹ IEEE 802.11a,g,n (CMW500)
Frequencies	Hardware supports up to 6 GHz Lab antennas: 698-960, 1710-2700, 2700-3200 MHz
Licenses	FCC experimental license, several bands in 450–3650 MHz range [28]
Channels	a) Channel emulation through cabled mode (RFnest) b) Over-the-air transmission with or w/o shielded enclosure
Synchronization	Eight 10 MHz and eight pulse per second (PPS) reference signals (Octoclock)
Access	Remote and physical

¹ Hardware, commercial software, and free open-source software

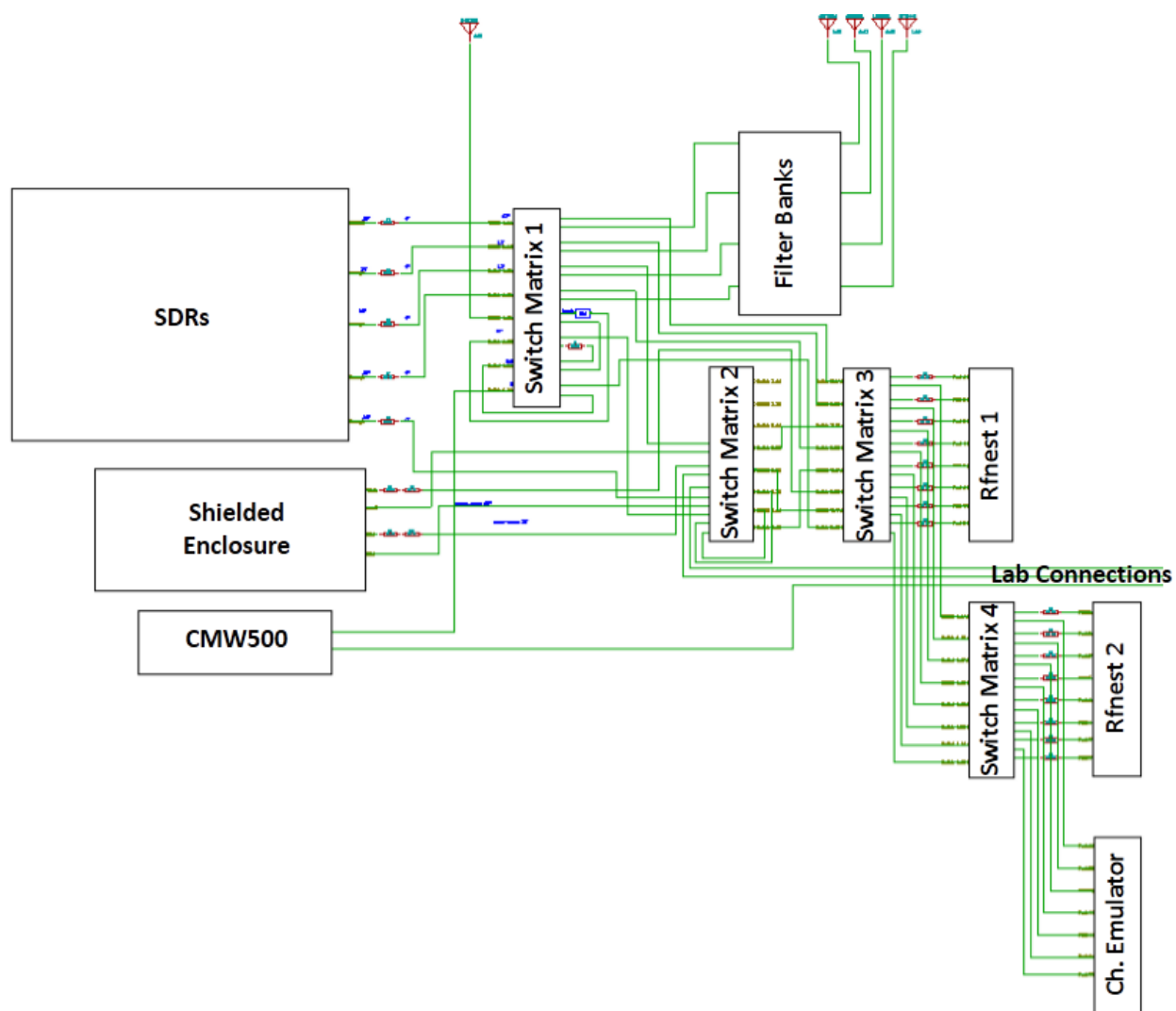


Figure 2. Functional RF diagram for all testbed operational modes including 2x2 MIMO.

3. Hardware

3.1 CMW500

The CMW500 from Rohde & Schwarz is a wideband communication system tester. Figure 3 shows a photo of the front panel. Our CMW500 is currently equipped with FD-LTE and TD-LTE firmware compliant with 3GPP Release 8. It allows monitoring LTE performance parameter, such as throughput, block error rate (BLER), and channel quality indicator (CQI), in real-time. Data logging is available for offline analysis. The CMW500 can also serve as a spectrum analyzer. Its main screen can be exported and all knobs and features remotely accessed and controlled.



Figure 3. Photo of CMW500.

Upgrades to newer 3GPP Releases or for adding functionalities are possible, but may require shipment to factory. The currently available features are summarized in Appendices J and M.

3.2 Computing Nodes

Several computing nodes provide the software processing capabilities of the testbed (Tables 1a-c). PCs 1-4 share a monitor that can be accessed locally through a KVM switch for system administration. The mobile workstations can be connected to the internal network of the fixed infrastructure or used individually. Another PC, not listed, serves as the gateway allowing remote access to the testbed (Section 5).

PC 5 is heavily used for simulations, whereas the rackmount workstation for emulating up to 64 LTE UEs. The three Intel NUC mini PCs serve dual purposes: (1) mobile SDR computing nodes and (2) hubs for powering, controlling, and accessing the LTE UE USB dongles described in Section 3.8.

Table 2a. Computer specifications (shaded columns indicate LTE-CORNET equipment).

	PC 1-3	PC 4 ¹	PC 5	Rackmount Workstation
Model	Dell Precision Tower 5810 Workstation	Dell Optiplex 9010	Dell Precision Tower 7810	Dell Precision R7910
Architecture	64 bit	64 bit	64 bit	64 bit
CPU	Intel Xeon Processor E5-1650v3 (6C, 3.5 GHz, Turbo, HT, 15M, 140W)	Intel Core i7-3770 (3.4 GHz Quad Core, 77W)	Dual Intel Xeon E5-2623 v3 (4C, 3 GHz) +GPGPU Nvidia Tesla K20C, 5GB	Dual Intel Xeon E5-2695 v4 (18C, 2.1GHz, 3.3GHz Turbo, 2400MHz, 45MB, 120W)
RAM	32GB (4x8 GB) 2133 MHz DDR4 RDIMM ECC	16GB (4x4GB) 1600MHz DDR3 DIMM	128 GB 2133 MHz DDR4 (8x16 GB)	128GB (8x16GB) 2400MHz DDR4 RDIMM ECC
Hard drive	256 GB SATA SSD 1 TB 7200RPM SATA HDD	500GB SATA 7200RPM HDD	Samsung 1TB 840 Evo SATA III SSD + 2TB 3.5" SATA HD	512GB Dell 4*Drive PCIe x16 M.2 SSD + 2.5" 512GB SATA Class 20 SSD
Video Card	NVIDIA Quadro NVS 310 512 MB (2 DP)	Intel IvyBridge Desktop	NVIDIA Quadro K2200 4 GB	Dual AMD FirePro™ W5100 4GB (4 DP) (4 DP to SL-DVI adapters)
Ports	2 Gigabit Ethernet 1+3 USB3 ports	2 Gigabit Ethernet 2+2 USB3 ports	1 Gigabit Ethernet 4 USB3 + 6 USB2	Quad Port Network Daughter Card (2x10GbE, 2x1Gbit) Intel X540

Table 2b. Computer specifications (shaded columns indicate LTE-CORNET equipment).

	Mobile Workstation 1	Mobile Workstation 2-6	Mobile Workstation 7-8
Name	LTE-DURIP	COMWITS1 - COMWITS5	comwits1-Precision-7510
Model	Dell Precision M4800 Workstation	M4800	Precision-7510
Architecture	64 bit	64 bit	64 bit
CPU	Intel i7-4910MQ (Quad core, 2.9GHz, 47W)	Intel i7-4910MQ	i7-6920HQ
RAM	16GB (4x4GB) 1600MHz DDR3 SODIMM	16 GB	32 GB
Hard drive	256GB 6.0 Gbps SATA SSD	256 GB	250 GB
Video Card	Gallium 0.4 on AMD Cape Verde	Intel Haswell Mobile	Nvidia Quadro M2200/PCIe/SSE2
Ports	1 Gigabit Ethernet 2+2 USB3 ports	1 Gigabit Ethernet 2+2 USB3	1 Gigabit Ethernet 2+2 USB3

¹ Available from another project

Table 2c. Computer specifications (shaded columns indicate LTE-CORNET equipment).

	Intel NUC-i5	Intel NUC-i7 (2)
Model	NUC5i5RYH	NUC6i7KYK
Architecture	64 bit	64 bit
CPU	Intel i5-5250U	Intel i7-6770HQ
RAM	8 GB	32 GB
Hard drive	Samsung 850 Evo 250 GB M.2 SSD	Samsung 950 Pro 256 GB M.2 SSD
Video Card	Intel HD Graphics 6000	Intel Iris Pro
Ports	1 Gigabit Ethernet 4 USB3	1 Gigabit Ethernet 3 USB3

3.3 Software Radio Peripherals

We use three N210s, ten B210 and three E310 Universal Software Radio Peripherals (USRPs) from NI/Ettus Research (Table 3). USRPs 1-3 are integrated in the fixed testbed located in 475 Durham Hall. USRPs 4-13 can be used with the fixed or mobile workstations, whereas USRPs 14-16 can be used autonomously or with a workstation. Figure 4 provides a configuration of the B210 with a host computer. Note that a host computer can process waveforms for several USRPs. Figure 5 shows four B210s and one N210 attached to a mobile workstation.

Table 3. USRP Specifications (shaded columns indicate LTE-CORNET equipment).

	USRP 1-3	USRP 4-5	USRP 6-13	USRP 14-16
Model	N210	B210	B210	E310
Interface	1000BaseT	USB3	USB3	USB console + USB2.0 + Gigabit Ethernet
IP address	192.168.10.2	-	-	-
UHD Version	3.5.4 and above	3.7.0 and above	3.7.0 and above	3.8.0 and above
Daughterboards	SBX (400-4400 MHz)	Integrated (100 MHz - 6 GHz)	Integrated (100 MHz - 6 GHz)	Integrated (70 MHz - 6 GHz)
Bandwidth	40 MHz	60 MHz	60 MHz	56 MHz
RF chains	1 TX/RX + 1 RX	2 TX/RX + 2 RX	2 TX/RX + 2 RX	
MIMO	No	2x2	2x2	2x2

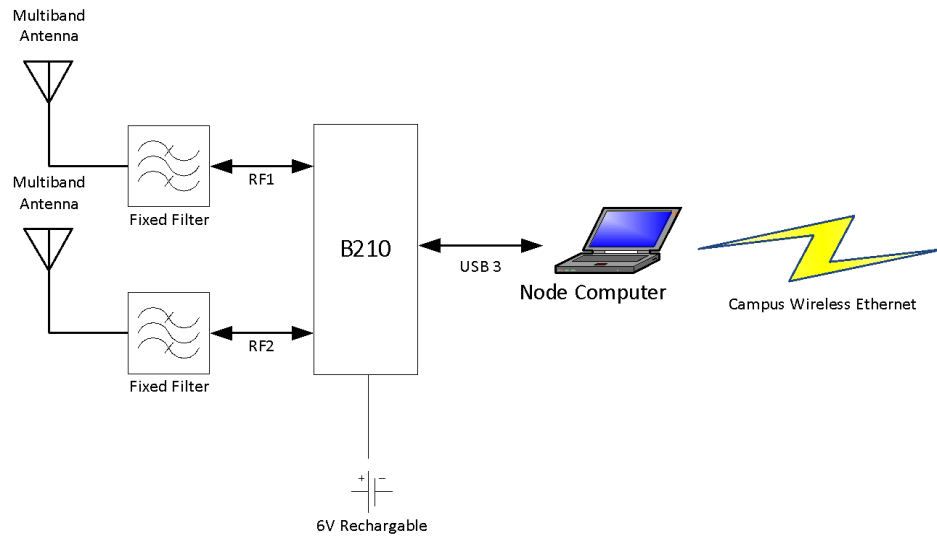


Figure 4. Mobile node with B210 USRP.

The Octoclock provides a common time reference. It is located in the lower part of the rack, underneath the three N210 USRPs and above the three PCs, as shown in Fig. 1.

```

student@ubuntu: ~
student@ubuntu:~$ uhd_find_devices
linux; GNU C++ version 4.8.4; Boost_105400; UHD_003.011.000.git-78-gf70dd85d

-----
-- UHD Device 0
-----
Device Address:
  type: b200
  name: MyB210
  serial: 30D3F40
  product: B210

-----
-- UHD Device 1
-----
Device Address:
  type: b200
  name: MyB210
  serial: 30D3F21
  product: B210

-----
-- UHD Device 2
-----
Device Address:
  type: b200
  name: MyB210
  serial: 30D3F46
  product: B210

-----
-- UHD Device 3
-----
Device Address:
  type: b200
  name: MyB210
  serial: 30D3F3F
  product: B210
  
```

Figure 5. Computing node with four B210 USRPs.

3.4 RF Processing

Each N210 USRP (USRP 1-3) has an RF processing block attached which consists of RF attenuators and combiners. The combiner takes the form of a wideband 10 dB directional coupler that allow both USRP ports to be used. The coupler through connection attaches to the USRP RX port. The coupled arm is connected to the USRP TX/RX port. This configuration provides 10 dB of attenuation to the transmitted signal while allowing for reception with no additional attenuation. An additional 10 dB attenuator is provided at the RFnest port to reduce the transmitted signal a total of 10 dB. Since the USRP N210 with SBX daughterboard can source 100 mW, the total attenuation of 20 dB provides approximately 0 dBm maximum signal to the RFnest port. The directional couplers are Mini-Circuits labs model ZHDC-10-63-S+ which have a specified frequency range of 50-6000 MHz.

A conventional 3 dB hybrid combiner is used to connect the TX/RX and RX ports of USRP 4.

3.5 Channel Emulator

Our testbed includes several channel emulators. We use the RFnest (Radio Frequency Network channel Emulation Simulation Tool) from Intelligent Automation, Inc. Figure 6 shows a photo. The channel emulator allows wireless nodes to experience realistic channel effects, and supports the integration of real radio nodes and virtual or simulator radio nodes. It comprises of four major components:

- **RFnest hardware:** The hardware carries out the digitization of the incoming RF signals, applies selected channel effects, generates RF signals digitally, and converts the resulting signals back to analog signals for all the connected radios in real-time. The model currently in use is the A208, and it allows up to 8 simultaneous RF connections, with support for up to 96 connections when cascaded with other RFnest hardware. The hardware communicates with other system components over the Ethernet interface.
- **RFview GUI:** It provides the user-interface for the system and allows for scenario modelling, analysis, and the recording and replay of scenarios. The GUI provides time-synchronized, geospatial graph-based displays of the scenario state, and the outcome of the scenario. Version 2.11 of the software is currently in use.
- **Channel Emulation Controller (CEC):** The CEC co-ordinates with the RFview and carries out initialization and updatation of properties as the scenario changes over time.
- **Channel models:** The system supports the following built-in channel models: free space model, Hata model (suburban, urban, rural), Hata PCS (suburban, urban), log distance model, and flat fading model. The present system does not support modelling of individual multipath delays and Doppler spread in the channel.



Figure 6. RFnest hardware showing the 8 RF ports and Ethernet interface.

Table 4. RFnest Specifications (bold frequencies are supported by our RFnest units).

Parameter	Specification
No. of ports	8
RF configuration	SISO, SIMO, MISO, MIMO, MESH
Frequency bands	0 - 1 GHz , 1.2-1.9 GHz, 1.8-2.8 GHz , 2.7 - 3 GHz, 3.4 - 4 GHz, 3.4 - 4 GHz
Dynamic Range	37 dB (1 dB resolution)
Input Power	<1 dBm
RF Output Level	-30 dB to -67 dB
RF Output Accuracy	2 dB
Maximum propagation delay	2 seconds
Doppler Shift	Up To 2 kHz

3.6 RF Filters

Our testbed provides support for over-the-air transmission as well as through RF cables. RF filter banks are connected between the RF switch and the antennas located in the RF Lab for use when the over-the-air mode is selected by the RF switch.

Since the USRP RF components (daughterboards) only includes a single fixed filter (cutoff at the highest specified daughterboard frequency of 4.4 GHz), it is evident that additional filtering must be provided in order to suppress transmitted harmonics and spurious receiver responses. Configurable filter banks are provided for use in conjunction with the antenna system for controlled over-the-air operation. One filter bank is dedicated to each fixed system USRP. The RF filter banks are not required when using the RFnest and settings can be ignored in that case.

The filter banks may be manually set by accessing the switch at its assigned IP number on a web browser. Initial filter frequencies and IP numbers are shown in Table 5. Filters can be exchanged for other filters to operate at other bands.

Table 5. Filter bank assignments.

Switch Position (A,B)	Filter Bank 1	Filter Bank 2	Filter Bank 3	Filter Bank 4
1,1	800-1000 MHz	800-1000 MHz	800-1000 MHz	800-1000 MHz
2,2	2025-2075 MHz	2025-2075 MHz	2025-2075 MHz	2025-2075 MHz
3,3	2350-2550 MHz	2350-2550 MHz	2350-2550 MHz	not defined
4,4	3550-3650 MHz	3550-3650 MHz	3550-3650 MHz	3550-3650 MHz
IP address	192.168.0.33	192.168.0.34	192.168.0.35	192.168.0.36
Other A,B combinations are invalid (disconnected).				

3.7 Antenna System

The system uses five ceiling mounted radome-enclosed, omni-directional, vertically polarized antennas operating over the range 698 - 6000 MHz. The antenna elements are procured from Galtronic Corporation Ltd., and the selected model is PEAR S4935i Pigtail – Broadband In-Building Omni Antenna. Each antenna is 1.65 lbs in weight, has a diameter of 13.2” and height of 4.88”. Figure 7 illustrates the antenna and Table 6 presents its electrical specifications. For a more detailed list of antenna specifications and performance parameters, please refer to the antenna datasheet available online at [3].



Figure 7. Omni-directional, ceiling mounted antenna [3].

Table 6. Electrical parameters of the antenna [3].

Parameter	Frequency Band			
	698-790 MHz	790-960 MHz	1710-2700 MHz	2700-3200 MHz
VSWR	< 1.5:1			
Gain	1.5-2.5 dBi	2.0-3.5 dBi	4.5-7.0 dBi	5.0-6.0 dBi
Input	N-type connector with pigtail cable			
Input impedance	50 ohms			
Input Power	50 W at ambient temperature of 25 deg C			

3.8 User Equipment

The following UEs are currently available as part of our testbed:

1. Huawei B593s-22 [32]
2. Huawei E3276 LTE Dongle [31]
3. Huawei E8278 [15]
4. Rogers Aircard U330 [30]

Figure 8 illustrates the form factors of these UEs and Table 7 provides the specifications. Each UE uses a test UICC subscriber identity module (USIM) from Rohde & Schwarz, CMW-Z04 Mini-UICC Test Card.

**Figure 8.** UEs.**Table 7.** UE Specifications.

	Rogers USB Dongle (2)	Huawei E3276	Huawei B593	Huawei E8278
Model	U330	E3276s-861	B593-s22	E8278
Interfaces	USB	USB	Ethernet USB	USB
LTE mode	FDD	TDD	FDD/TDD	FDD/TDD
LTE bands	Band 3, 4, 7 and 17	Band 38	Band 1, 5, 7,8, 9 (FDD); 38 (TDD)	Band 1, 5, 7,8, 9 (FDD); 38 (TDD)
Built-in antenna	Yes	Yes	Yes	Yes
MIMO	Yes [11]	Yes	Yes	Yes

3.9 Spectrum Analyzer

The testbed includes two portable spectrum analyzers - the Tektronix SA2500 for indoor and outdoor measurement studies over a frequency range of 10 kHz - 6.2 MHz. It is a mobile unit that can be hooked up with the testbed as needed. An example scenario for OTA testing in the RF lab, it could be used for measurements along with the mobile nodes. The spectrum analyzer supports remote operation using its LAN interface, and its built-in GPS receiver allows location information to be exported alongside spectrum data. The SA has a GPS receiver. For a complete list of specifications, please refer to its datasheet available online [2]. Figure 9 shows a screenshot of two experimental LTE downlink signals generated by our testbed and captured by our spectrum analyzer integrated into our system through RF cables.

3.10 Reference Oscillator and Clock Source

Ettus Research Octoclock. It has eight 10 MHz and eight 1 pulse per second reference signals. It distributes a common timing (1 pps) and 10 MHz reference signal to the USRPs and CMW500. The use of it is optional. You can select through the USRP hardware driver (uhd) whether to use an internal or external reference signals. Octoclock allows to provide an increase in frequency accuracy. The 1 pulse per second (1 pps) signal allows the sample clocks to be aligned.

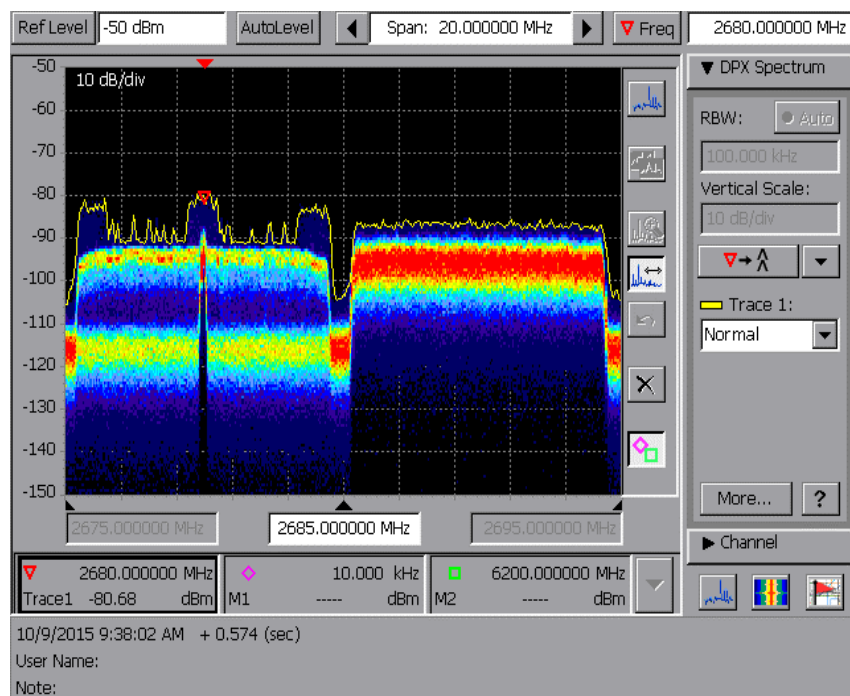


Figure 9. RF Spectra of two adjacent 10 MHz LTE cells. The left band shows a TD-LTE signal spectrum, generated by the Amarisoft LTE100 eNB with N210 USRP. The power level histogram shows peaks at -95 and around -117 dBm because of the different received power levels of the UL and DL signals. We also see the SDR's local oscillator leakage at the carrier frequency at 2680 MHz. The right band shows a clean FD-LTE downlink signal spectrum, generated by the CMW500, with full resource allocation.

3.11 RF Switches

LTE-CORNET provides support for over-the-air transmission as well as through RF cables. A switch allows switching between the cabled mode, going through the channel emulator, and the over-the-air transmission going through filters. The default RF switch settings (Position 1) connect the USRPs and CMW500 to RFnest. By connecting switch sections A - D to Position 2, the antennas are selected. Switch sections G and H may be used in concert to connect either the CMW500, Antenna 5 or Lab Cable 7 to the RFnest. Table 8 describes the switch settings. The RF switch may be manually set by accessing the switch at its assigned IP number (192.168.0.30) on a Web Browser.

Table 8. RF Switch Settings.

Switch Section	Common terminal	Position 1 (default)	Position 2
A	USRP 1	RFnest port 0	Antenna 1
B	USRP 2	RFnest port 1	Antenna 2
C	USRP 3	RFnest port 2	Antenna 3
D	USRP 4	RFnest port 3	Antenna 4
E	not defined	not defined	not defined
F	not defined	not defined	not defined
G	CMW500 in/out	RFnest port 8*	Cable 7 to lab
H	RFnest Port 8	CMW500 in/out*	Antenna 5

*only for 7A and 8A otherwise no connection

4. Software

Tables 8a-c summarize the software installed on the processing nodes of the COMWITS/LTE-CORNET.

Table 9a. Software installed on processing nodes (shaded columns indicate LTE-CORNET equipment).

	PC1	PC2	PC3	PC4 ¹	PC 5	Rackmount Workstation
User name	ltecornet1	ltecornet2	ltecornet3	wireless	wireless	ltecornet5
Operating System	Ubuntu 14.04 LTS	Ubuntu 14.04 LTS	Ubuntu 14.04 LTS	Fedora 20 (Heisenberg)	Windows 10	Ubuntu 14.04 LTS
UHD	3.8.1	3.5.4	3.5.4	3.5.4	-	3.8.1
GNU Radio	3.7.6.1	3.7.0	3.7.0	-	-	-
Amarisoft	June 1st, 2015 (3GPP Rel. 12)	-	-	January 20th, 2015 (3GPP Rel. 12)	-	June 23rd, 2016; Amarisoft 64 UE Emulator
srsLTE	-	yes	yes	-	-	-
OAI	-	yes	yes	-	-	-
RFnest	yes (RFveiw version 2.11)	-	-	-	-	-
Matlab	-	-	-	-	Yes	-

¹ Available from another project.

Table 9b. Software installed on processing nodes (shaded columns indicate LTE-CORNET equipment).

	MW1 ²	MW2	MW3	MW4	MW5	MW6
User name	lte-durip	COMWITS1	COMWITS2	COMWITS3	COMWITS4	COMWITS5
Operating System	Ubuntu 14.04 LTS	Ubuntu 14.04 LTS	Ubuntu 14.04 LTS	Ubuntu 16.04 LTS	Ubuntu 16.04 LTS	Ubuntu 16.04 LTS
UHD	3.7.0	3.11.0 ¹	3.11.0 ¹	3.9.4	3.9.4	3.9.4
GNU Radio	3.7.5	3.7.10.1 ¹	3.7.10.1 ¹	3.7.9	3.7.9	3.7.9
Amarisoft	3GPP Rel. 9 and 12	-	-	-	-	-
srsLTE	yes (libLTE)	-	-	-	-	-

¹ On Ubuntu host virtual machine accessed via VMware Player

² Mobile workstation (MW)

Table 9c. Software installed on processing nodes (shaded columns indicate LTE-CORNET equipment).

	MW7 ²	MW8	NUC-i5	NUC-i7-1	NUC-i7-2
Operating System	Ubuntu 14.04 LTS	Ubuntu 14.04 LTS	Windows 7 + Ubuntu 14.04 LTS	Windows 7	Windows 10
UHD	3.11.0 ¹	3.11.0 ¹	-	-	-
GNU Radio¹	3.7.10.1 ¹	3.7.10.1 ¹	-	-	-
Huawei UE Software	-	-	Yes	Yes	-

¹ On Ubuntu host virtual machine accessed via VMware Player² Mobile workstation (MW)

4.1 Wireless Communications Software

4.1.1 Amarisoft

Amarisoft Software LTE eNodeB is installed currently on several workstations, on two fixed and one mobile workstation. It supports operation with USRPs B210 and N210. Whereas N210 needs a UHD version greater than 3.5.0, B210 needs a UHD version 3.7.0 or greater. Any UHD version that does not satisfy these are incompatible with Amarisoft. In the tests that have been carried out so far, Amarisoft is able to connect to 2 UEs.

4.1.2 Amarisoft UE Emulator

Amarisoft's 64 UE Emulator allows up to 64 UEs to be emulated and controlled through a GUI interface. It is installed and tested on the rackmount workstation.

4.1.3 srsLTE

srsLTE (formerly libLTE) is an open-source and free SDR library for implementing 3GPP compliant LTE system on PCs connected to USRPs. It has a modular structure with minimal inter-modular and external dependencies. The current version is compliant with LTE Release 8, and is written entirely using C language. For more information, refer to the documentation in the website of the srsLTE project at [4].

4.2.4 Open Air Interface

The OpenAirInterface Software Alliance (OSA) is a French non-profit organisation that provides a standard-compliant implementation of a subset of Release 10 LTE for Linux-based general purpose computers. It is freely distributed by the Alliance and can be used with Ettus USRPs and PXIe platforms, in addition to custom hardware from EURECOM. More details about the OSA initiative can be found on their website at [5].

4.2.5 GNU Radio

GNU Radio is a free and open-source software development kit meant for implementing and rapid prototyping of DSP algorithms for SDR. It can be used with a) low-cost external RF hardware to create a software radio, or b) used without any external hardware in a purely simulation-based setting.

GNU Radio companion (GRC) is installed on most workstations. To install GNURadio, it is recommended to use a version of UHD that is compatible with both Amarisoft and GNU Radio. UHD version 3.8.1 is running on this system, that has been found to be compatible with all other software tools.

GNU Radio version 3.6, including GNU Radio Companion (GRC), is installed on most nodes. The mobile nodes M1 and M2 run the latest GNU Radio version, version 3.7. Upgrades to newer versions are planned based on the needs. We recommend using the build-gnuradio script available at [6]. See also the GNU Radio Web site for more information, tutorials and related links.

4.2 Performance Analysis Software

4.3.1 iPerf

iPerf is a measurement tool that creates streams of traffic data and determines the maximum achievable bandwidth on IP networks. It is originally developed by ESnet/Lawrence Berkeley National Laboratory and is available for download from its homepage at [9].

4.3.2 jPerf

jPerf is a GUI front-end developed in Java for iPerf. It provides an interface to select various options, which are ultimately translated to a command line interface.

5. Networking and User Access

Users access the testbed remotely. Users can register and reserve the testbed for a reasonable duration. If approved, the single user or user group is granted exclusive access to the tested for the defined period. Table 10 and Fig. 10 show the networking specifications and the network layout. The IP-based network allows remotely accessing and controlling the different components of the system. The following sections describe the user access mechanism in more detail.

Table 10. Networking specifications.

Computer/Device	MAC Address	IP Address 1	IP Address 2	Access software
Gateway	----	192.168.0.1	128.173.94.254	OpenVPN
PC 1	eth0 - a0:36:9f:5e:c4:19 eth1 - 98:90:96:9c:be:24	192.168.10.1	192.168.0.11	VNC server
PC 2	eth0 - a0:36:9f:5e:c1:ac eth1 - 98:90:96:9c:c1:8c	192.168.10.1	192.168.0.12	VNC server
PC 3	eth0 - a0:36:9f:5e:c5:13 eth1 - 98:90:96:9c:bf:d7	192.168.10.1	192.168.0.13	VNC server
PC 4 (Fedora PC)	----	192.168.10.1	N/A	----
Mobile workstation	eth0 - 00:0a:cd:21:49:8a eth1 - 34:e6:d7:06:38:53 wlan: 80:19:34:60:29:q8	192.168.10.1	N/A	----
CMW 500	----	192.168.0.14	----	Remmina
USRP 1-3	----	192.168.10.2	----	----
RF Switches 1-7	----	192.168.0.30-37	----	----
RF Attenuators 1-7	----	192.168.0.40-47	----	----

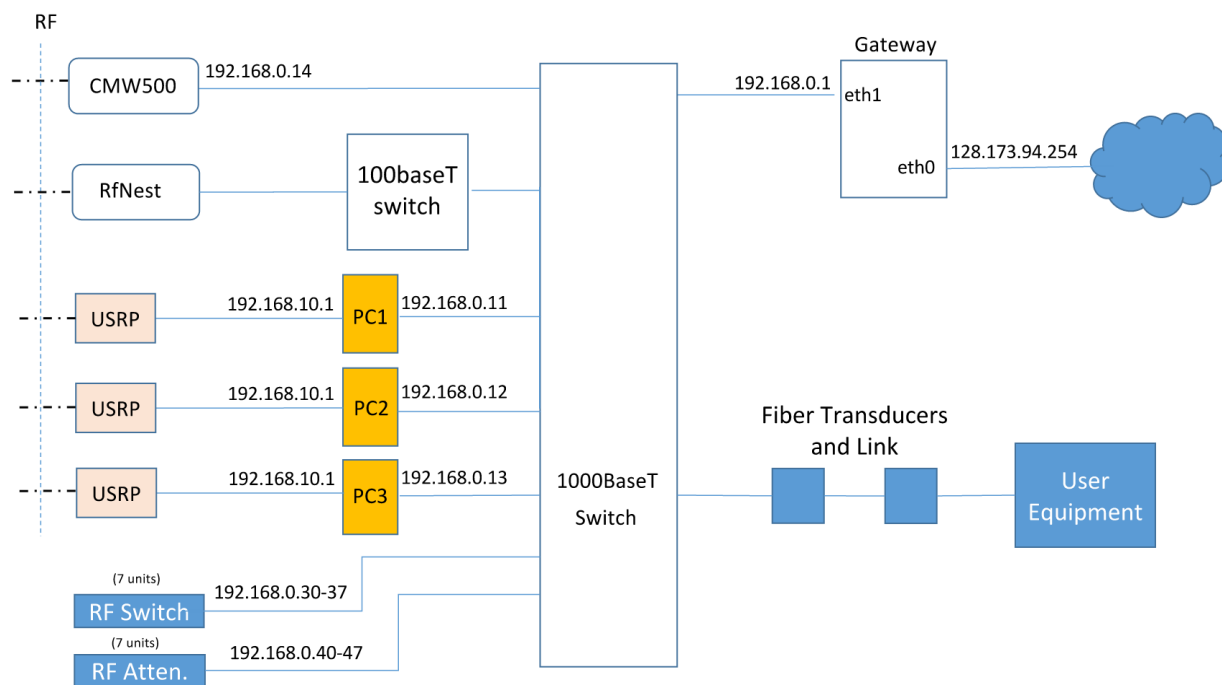


Figure 10. Internal network layout.

6. User Manual

6.1 User Registration and General Usage Instructions

Each testbed user is required to obtain a *username* and *password* from the system administrators. Users will be required to sign a user agreement that outlines their responsibilities and duties towards the operation of the testbed.

Being a specialized experiment environment, users should familiarize themselves with a few important ideas:

- As with the operation of any radio equipment, there is always the possibility of accidentally creating harmful interference to other spectrum users. Hence, it is necessary for the testbed users to always be aware and considerate of other users and always consult the frequency plan before transmitting over-the-air.
- In normal operation, a user would not be required to update/install any software package on the systems. There are complex interactions/dependencies between the various software modules installed on the testbed computers, and any attempt at updating/modifying may break some functionality. The user should consult with the system administrator if additional software is needed.
- Any data generated by a user and stored on the systems would be the user's responsibility, and would have to be backed up elsewhere. All system components can be reimaged and reset to the original state after the end of a user's approved experiment duration and the administrators would not be responsible for any data loss. Users are requested to work with the administrators towards data management and efficient utilization of system resources.

6.2 Accessing the Testbed

The testbed can be accessed remotely by authorized users over a Virtual Private Network (VPN) by using a valid .OVPN certificate that was issued by the testbed administrator. The certificate is verified by the gateway computer, and once authenticated, users are granted access to the networked system components.

After obtaining an .OVPN certificate, the user would have to setup the OpenVPN software to access the testbed as follows:

- For Windows Users:
 1. Download and install the OpenVPN Windows Installer (64-bit) here: <http://openvpn.net/index.php/open-source/downloads.html>
 2. During the OpenVPN install, accept the default options, and install the TAP-Windows device software when prompted.
 3. Create and download your OpenVPN certificate here: <https://cor.net.wireless.vt.edu/vpn>
 4. Move your ovpn file (<pid>.ovpn) to the C:\Program Files\OpenVPN\config folder

5. Right click on the OpenVPN GUI icon on your desktop and select Properties
 6. Open the Compatibility tab
 7. Under Privilege Level, check the box for "Run this program as an Administrator" and click OK
 8. Open OpenVPN GUI
 9. You should now see a new network icon in the system tray on the lower right. Right click and select Connect
- For OS X Users:
 1. Download and install Tunnelblick
 2. Create and download your OpenVPN certificate here: <https://cornet.wireless.vt.edu/vpn>
 3. Double click your ovpn file (<pid>.ovpn) to install
 4. Select the Tunnelblick icon in the top right of the menu bar and connect

After setting up OpenVPN correctly, and connecting to the testbed using the certificate, users should be able to notice a 10.25.0.* IP address in their list of IP addresses. (*for windows: ipconfig /all, *nix: ifconfig*)

Note that at this stage, the user has successfully connected to the main network switch of the testbed, and his or her computer would behave as if it was physically on the same network as the testbed components. The next step is to access the PCs for running the software, and have their GUIs displayed on the user's computer. These two steps are accomplished by using the software packages of PuTTY and TightVNC respectively.

6.2.1 PuTTY

PuTTY is an open-source SSH and telnet client for the Windows platform that is developed and supported by a group of volunteers. It was developed originally by Simon Tathan, and can be downloaded from [7].

Once connected over the VPN, Windows users may use PuTTY to access any of the three testbed computers as follows:

1. Open a PuTTY session (or similar utility). Enter the testbed computer's IP address and SSH.
2. When a terminal window opens you should see a login prompt. Enter your assigned user name.
3. Enter your password at the prompt. You will get a welcome screen. Do not run upgrades!
4. This is a command line on the testbed computer. You will have user and limited sudo privileges. Using TightVNC Viewer (described in the next section), users would be able to work with software GUIs.
5. To exit, halt all user programs and logout. Caution: Do not use "Shutdown" with no options from the command line. This will disable the node and require restarting it physically.

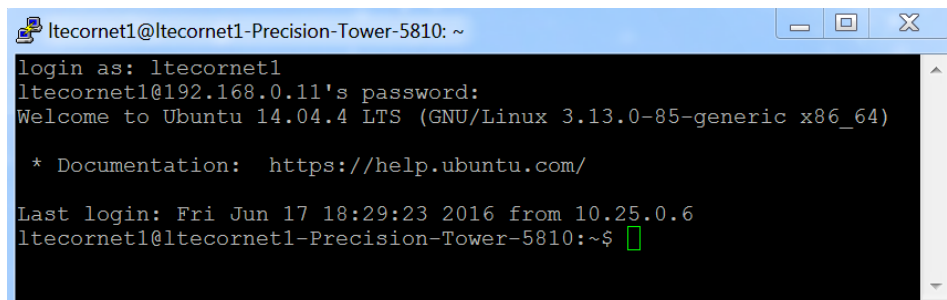
A screenshot of a PuTTY terminal window. The title bar reads "ltecornet1@ltecornet1-Precision-Tower-5810: ~". The terminal text shows a login sequence: "login as: ltecornet1", "ltecornet1@192.168.0.11's password:", and a welcome message "Welcome to Ubuntu 14.04.4 LTS (GNU/Linux 3.13.0-85-generic x86_64)". It also includes a link to documentation "https://help.ubuntu.com/", the last login time "Last login: Fri Jun 17 18:29:23 2016 from 10.25.0.6", and a command prompt "ltecornet1@ltecornet1-Precision-Tower-5810:~\$" with a green cursor.

Figure 11: Example SSH (putty) login screen and command prompt.

6.2.2 TightVNC Remote Desktop

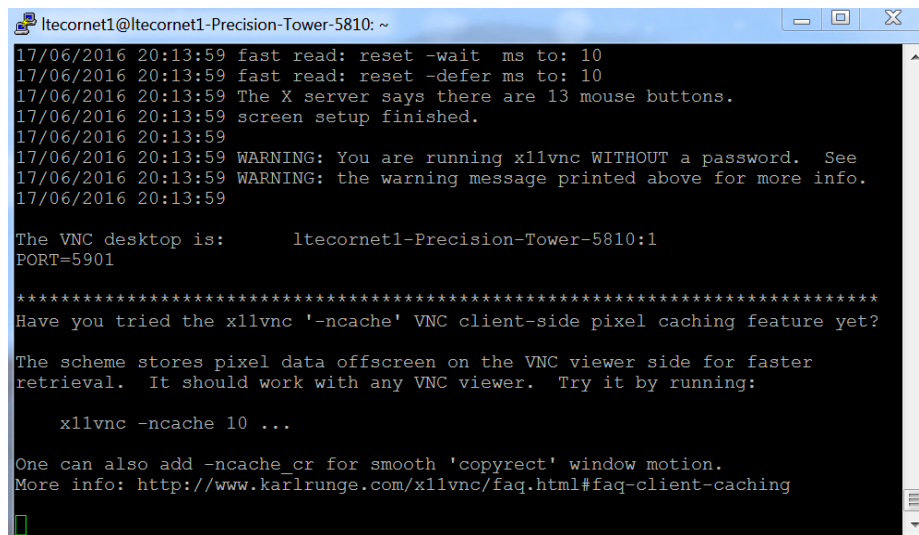
TightVNC is an open-source software allowing remote desktop export based on ssh. It allows one to control a remote machine with a local mouse and keyboard just like a user sitting in front of that computer.

Once the user has used PuTTY to access the testbed computers, the GUI screen can be accessed using TightVNC as follows:

1. At the command prompt, type the following:

```
$ x11vnc
```

This launches the remote desktop server on the machine, and the terminal window displays confirmation messages and a port number for the machine.



```
ltecornet1@ltecornet1-Precision-Tower-5810: ~
17/06/2016 20:13:59 fast read: reset -wait ms to: 10
17/06/2016 20:13:59 fast read: reset -defer ms to: 10
17/06/2016 20:13:59 The X server says there are 13 mouse buttons.
17/06/2016 20:13:59 screen setup finished.
17/06/2016 20:13:59
17/06/2016 20:13:59 WARNING: You are running x11vnc WITHOUT a password. See
17/06/2016 20:13:59 WARNING: the warning message printed above for more info.
17/06/2016 20:13:59

The VNC desktop is:      ltecornet1-Precision-Tower-5810:1
PORT=5901

*****
Have you tried the x11vnc '-ncache' VNC client-side pixel caching feature yet?

The scheme stores pixel data offscreen on the VNC viewer side for faster
retrieval. It should work with any VNC viewer. Try it by running:

    x11vnc -ncache 10 ...

One can also add -ncache_cr for smooth 'copyrect' window motion.
More info: http://www.karlrunge.com/x11vnc/faq.html#faq-client-caching
```

Figure 12: Example command screen showing port number displayed after running `$ x11vnc`

2. If not installed, users would have to install a VNC client on their computer. TightVNC has been tested extensively for accessing the testbed computers. It can be downloaded from [8].
3. Next, open the TightVNC Viewer and for the Remote Host, use the IP address of the testbed computer and the port number displayed earlier in the format: *ip_address :: port_number* and hit 'Connect'.

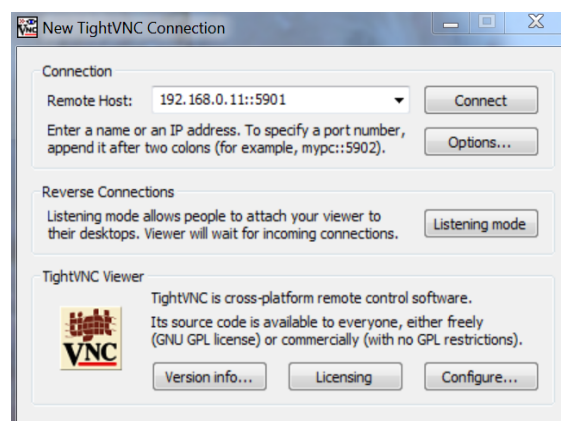


Figure 13: Sample TightVNC Viewer screen

4. You should be viewing the remote desktop.
5. To exit the session, close your user software and exit Tight VNC.
6. Return to the terminal or putty and close your vnc session by using the command:

```
$ x11vnc -kill
```

6.2.3 Example of accessing the testbed

This section presents a screen-by-screen visual summary of the steps outline above for remote access of the testbed. After successfully completing this procedure, launching and remote operation of the CMW500 is also presented as an example. For each screen, the relevant menus and options are highlighted by a green outline for clarity.

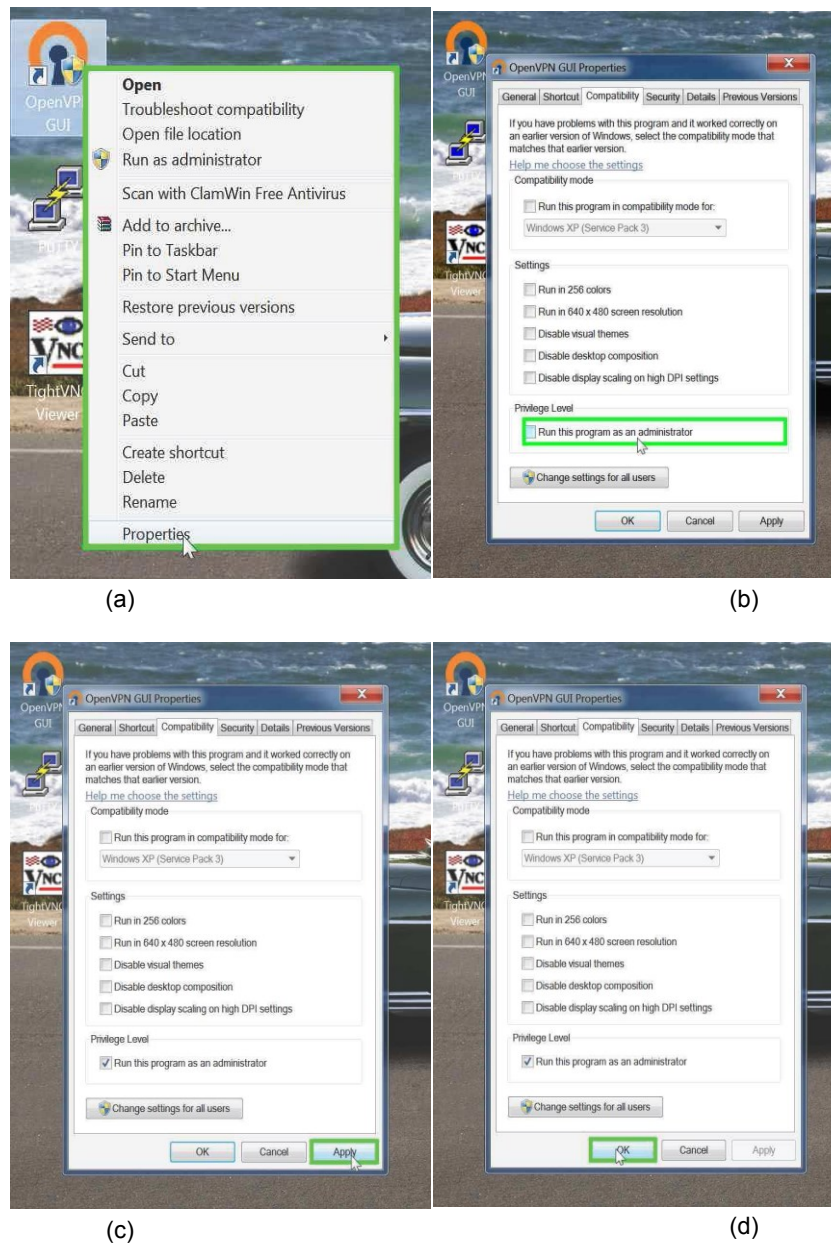


Figure 14a-d: Ensuring OpenVPN software has administrator privileges.

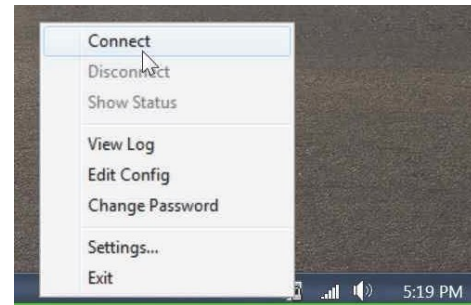
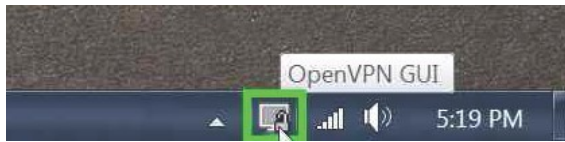


Figure 15a,b: Connecting using OpenVPN.

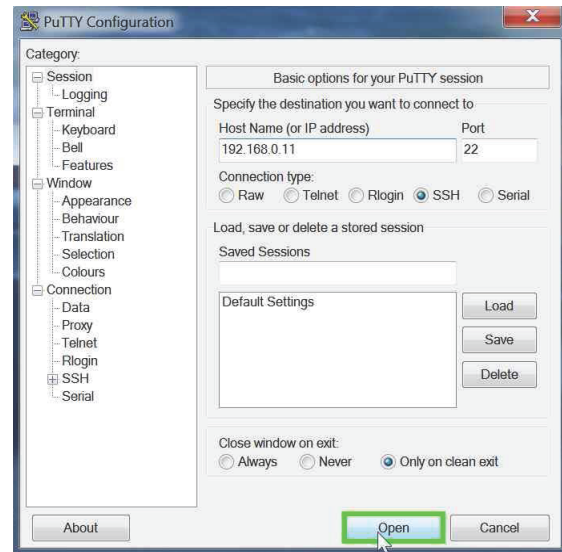
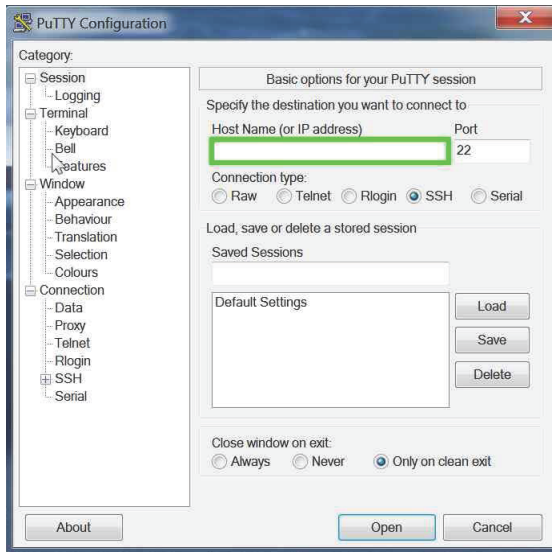


Figure 16a,b: Launching PuTTY.

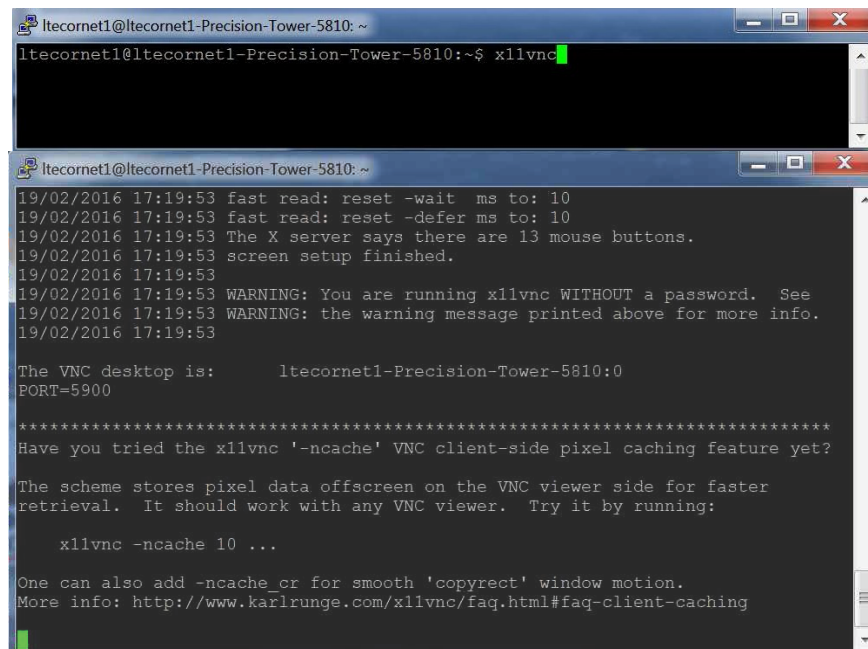


Figure 17a,b: Launching the remote desktop server.

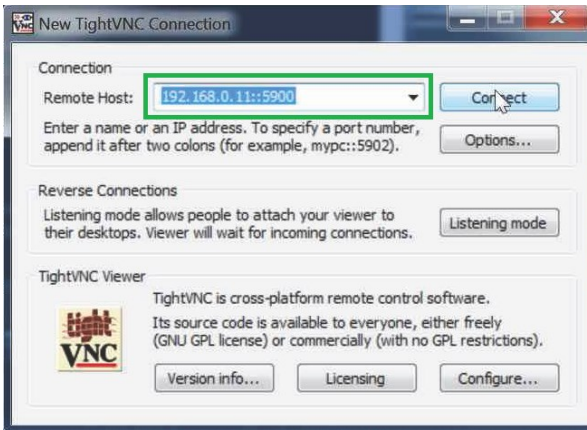


Figure 18: Launching TightVNC Viewer.

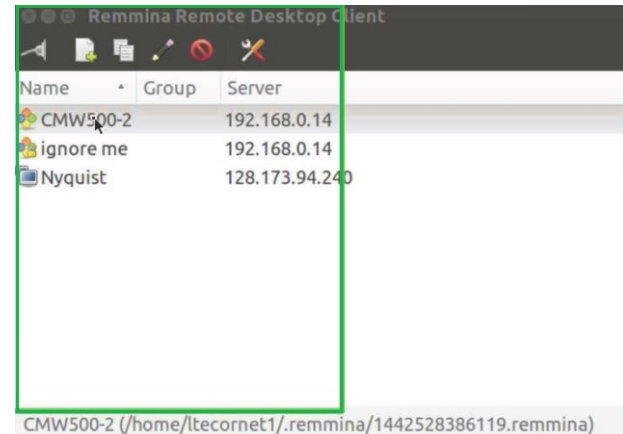


Figure 19: Launching Remmina to connect to CMW500.

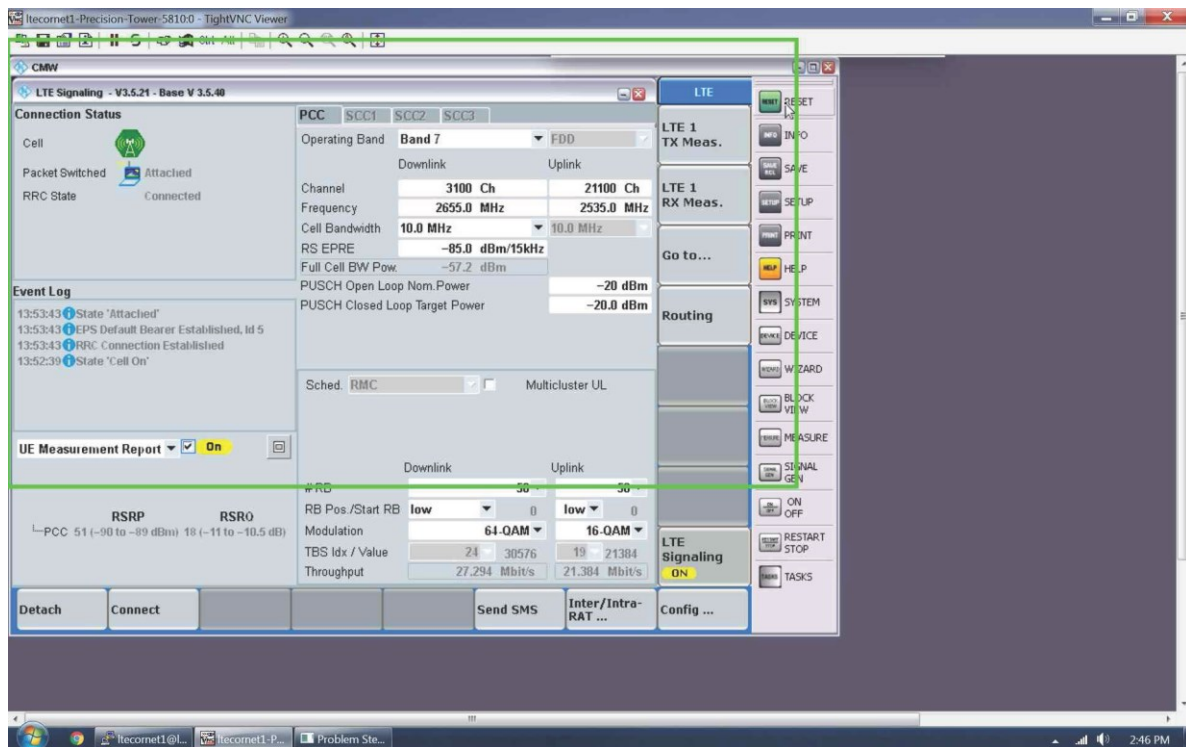


Figure 20: The CMW500 interface.

6.3 Configuring the Testbed

This section describes the steps involved in using the various testbed for deploying a LTE base station, core network and channel emulator scenarios. For a more detailed discussion, the user is encouraged to refer to the specific documentation for the particular software or hardware component.

6.3.1 Amarisoft

Amarisoft's Amari LTE 100 is a software eNodeB + Evolved Packet Core Network. It gives a powerful computer interfaced with a USRP, the capability to form its own LTE Evolved Packet Core Network. This section describes the procedure of installing the software package, and on using it.

The two most important modules of Amarisoft that the user needs to be aware of are

1. LTEENB: This module implements the radio front-end of the eNodeB on the USRP interfaced to the computer. The USRPs currently in use, in the testbed are B210s and the N210s.
2. LTEMME: The module emulates the Mobility Management Entity (MME) + Evolved Packet core of the LTE network.

Installing Amarisoft on an Ubuntu Machine

1. Install dependencies, especially for Stream Control Transmission Protocol (SCTP) as this is how the USRPs communicate with the machine.

```
sudo apt-get install lksctp-tools linux-image-extra-3.13.0-24-generic.
```

Some symbolic links may be necessary due to naming differences between Fedora and Ubuntu:

```
$ls -s /lib/x86_64-linux-gnu/libcrypto.so.1.0.0 /lib/x86_64-linux-  
gnu/libcrypto.so.1.0  
$ln -s /lib/x86_64-linux-gnu/libssl.so.1.0.0 /lib/x86_64-linux-  
gnu/libssl.so.1.0
```

2. Install UHDS (USRP Hardware Driver). To run Amarisoft with
 - a. USRP N210 - UHD version 3.5.4 and above.
 - b. USRP B210 - UHD version 3.7.0 and above.

Advisable to do a source installation of the UHDS. Follow the procedure in http://files.ettus.com/manual/page_build_guide.html under sections “Getting the source code”, “Build Instructions (UNIX)” and “Post-install tasks”.

3. Install Amarisoft by getting the license keys. The license keys are obtained by running

```
$sudo ./ltemme config/mme.cfg
```

or

```
$sudo ./lteenb config/enb.cfg
```

The node-locked license presents a 16-digit hexadecimal code that needs to be sent to support@amarisoft.com. Once the keys are obtained, of names ‘ltemme.key’ and ‘lteenb.key’. Create a folder .amarisoft in the home directory of the root user and copy these keys in the folder:

```
$su  
$cd /root/  
$mkdir ./amarisoft  
$cp {Folder where the keys are present} /root/.amarisoft/
```

4. Set up IP forwarding and masquerading on the PC. The script for doing so is written in ‘lte_init.sh’. Not setting this up would prevent the UEs from being able to access the internet.

Using Amarisoft

The most common applications of Amarisoft involve execution of the LTEENB (eNodeB) and LTEMME (Mobility Management Entity) modules. The most basic configuration for testing Amarisoft is by executing

```
$sudo ./ltemme config/mme.cfg
```

and in another terminal, executing

```
$sudo ./lteenb config/enb.cfg
```


Care must be taken to ensure that the appropriate configuration files are used in 'enb.cfg'. For USRP B210, it is "rf_driver-1chan-b2x0.cfg" and for N210, it is "rf_driver-1chan.cfg".

There are a lot of parameters that can be changed in the configuration file. For detailed information, read the Amarisoft documentation on LTEENB.

It is possible to connect multiple USRPs to the same PC running Amarisoft, constrained by the number of Ethernet (for the N210) and the USB (for the B210) ports and the computational power of the PC. This is possible by the following sequence of steps

1. Changing the GTP-U addresses in the specific configuration files,
2. adding the USRP device serial number in the driver configuration file for the USRP, i.e. "rf_driver-1chan-b2x0.cfg" and for N210, it is "rf_driver-1chan.cfg".

More details about connecting multiple USRPs to the same machine is provided in the cheat sheet.

6.3.2 RFnest

The RFnest hardware uses two software modules for executing different scenarios - the Channel Emulator Controller (CEC), and the RFView GUI. The GUI provides a visual environment to define the parameters of the scenario, and the CEC acts as the interface with the hardware. Hence, it is always a good practice to first launch the CEC, followed by the GUI each time the attenuation values between the ports are to be modified. With the CEC running in the background, the RFView GUI should be launched through a separate terminal window. This section describes the steps required to access the RFView GUI and CEC. For specific instructions on creating and modifying scenarios using the GUI, the user should consult the RFnest documentation and examples contained in them.

The procedure for launching CEC and RFView GUI is as follows:

1. Navigate to the CEC installation folder by typing the following command in a terminal window

```
$ cd Desktop
$ cd cec
```

2. The next step is launching the CEC script. This is done by the command,

```
$ ./run.sh
```

3. Once CEC is running, its version number is displayed in the terminal. Closing the terminal window will exit CEC, and it is recommend to use a separate terminal window for launching other programs.

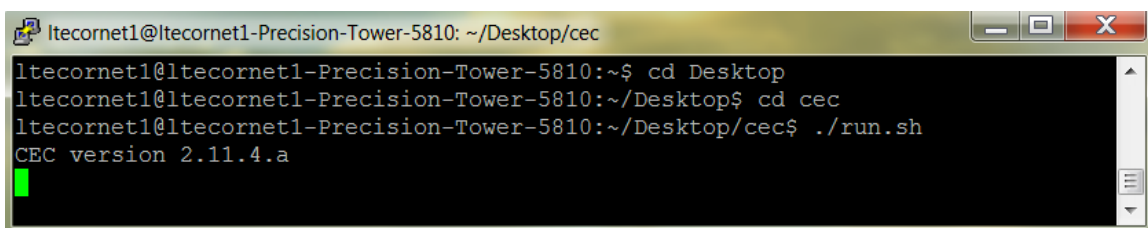


Figure 21: Launching CEC using the terminal.

The procedure for launching RFview GUI is as follows:

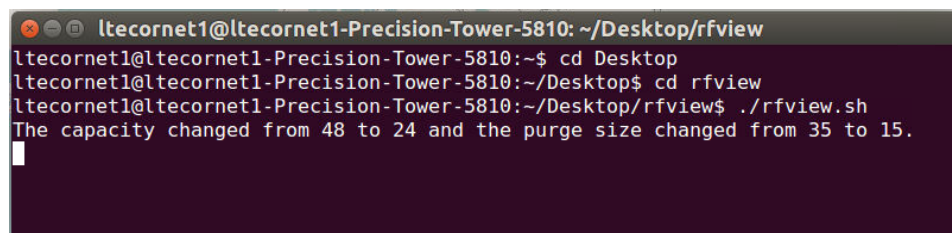
1. Navigate to the RFnest installation folder by typing the following command in a terminal window

```
$ cd Desktop
$ cd rfview
```

2. The next step is launching the RFview script. This is done by the command,

```
$ ./rfview.sh
```

3. Once launched, the terminal window displays a confirmation message and the GUI is launched. Use the RFnest documentation to configure and modify scenarios using the GUI.



```
ltecornet1@ltecornet1-Precision-Tower-5810: ~/Desktop/rfview
ltecornet1@ltecornet1-Precision-Tower-5810:~$ cd Desktop
ltecornet1@ltecornet1-Precision-Tower-5810:~/Desktop$ cd rfview
ltecornet1@ltecornet1-Precision-Tower-5810:~/Desktop/rfview$ ./rfview.sh
The capacity changed from 48 to 24 and the purge size changed from 35 to 15.
```

Figure 22: Launching RFview script using the terminal.

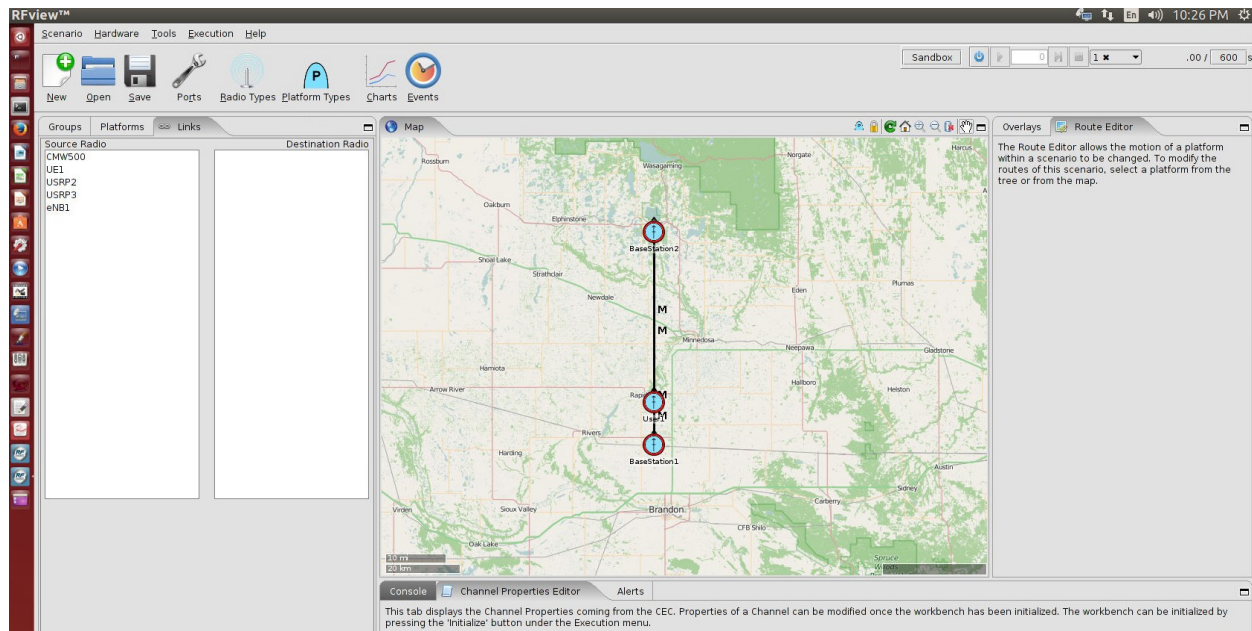


Figure 23: RFview GUI showing a loaded scenario.

4. At any time, pressing the button next to the 'Sandbox' option on the menu bar initializes the system. If at the end of the initialization process, an error is displayed instead of a confirmation message, check if the hardware is powered ON and if CEC is running correctly.

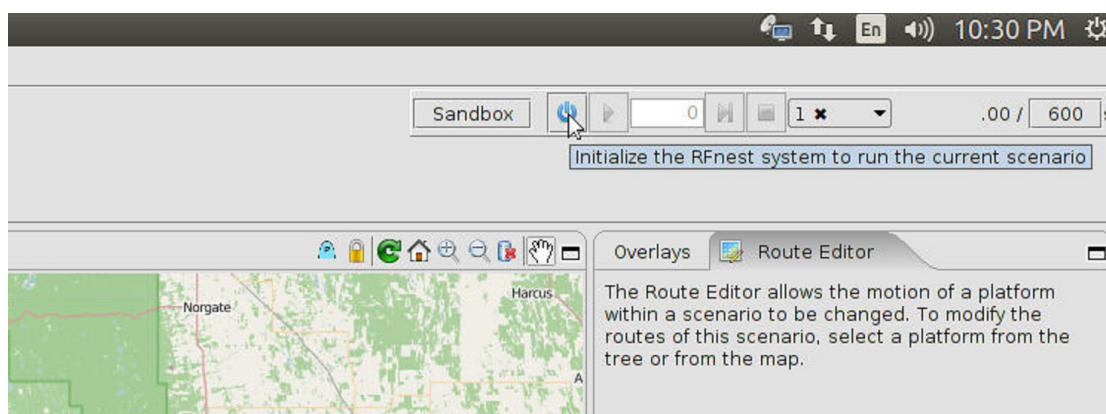


Figure 24: Initializing the RFnest hardware using RFview GUI.

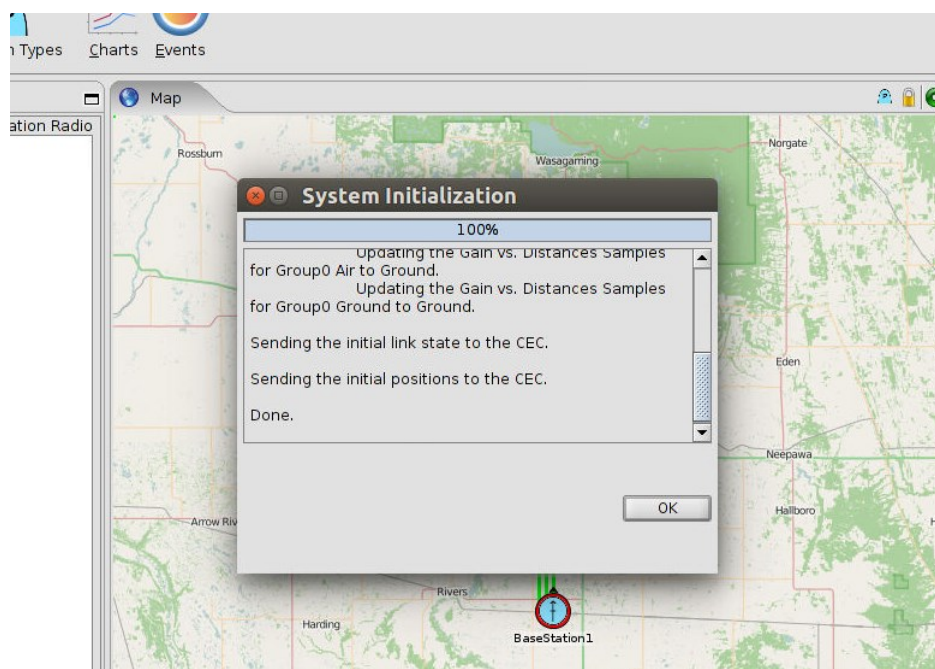


Figure 25: Confirmation message displayed after successful initialization of the RFnest hardware.

6.3.3 CMW500

The procedure for accessing the CMW500 instrument is outlined in an example in the earlier section. For specific instructions on setting up an eNodeB, modifying parameters, accessing performance parameters etc. the user may please refer to the CMW500 User Guide and White Papers available online on the Rohde & Schwarz website.

It is always a good practice to reset the CMW500 at the start of an experiment session. This ensures that all parameters are configured as per the requirements of the current experiment, and eliminates the accidental use of an earlier configuration.

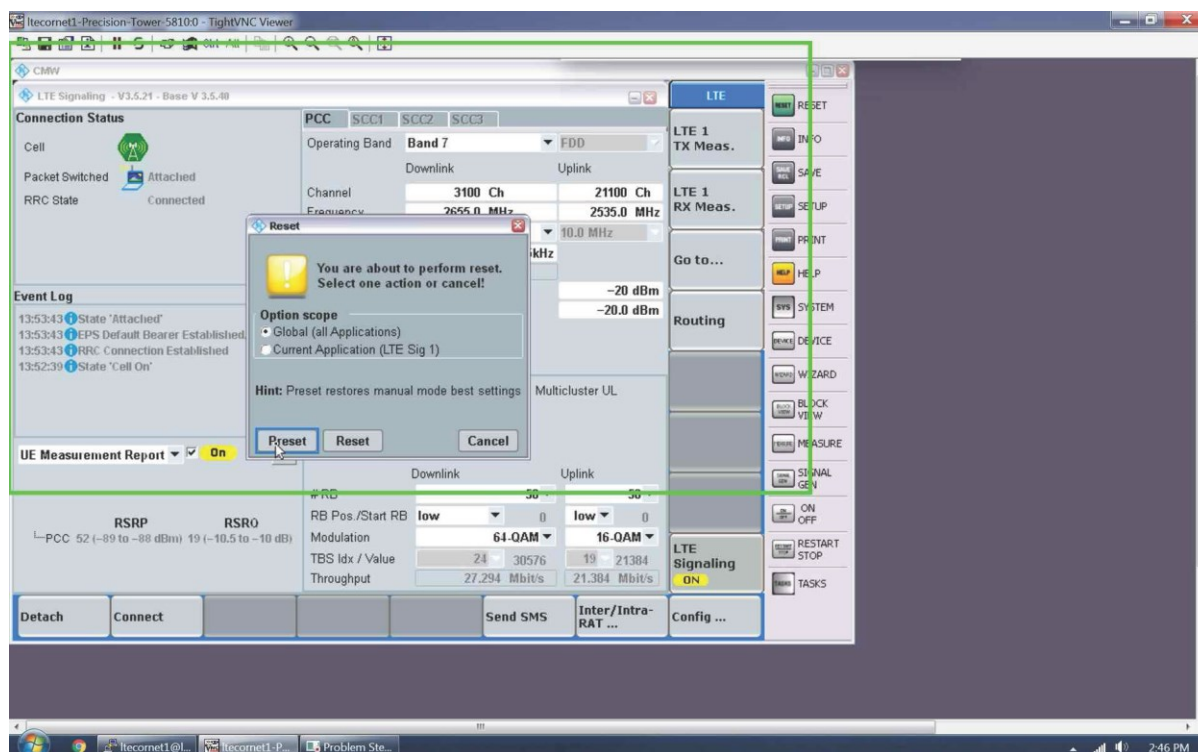


Figure 26: Performing a reset on the CMW500 prior to an experiment.

Also, if not being used for an extended duration of time, it is a good practice to turn off the signal generators on the CMW500. This helps in conserving power and also prolongs the life of the RF hardware.

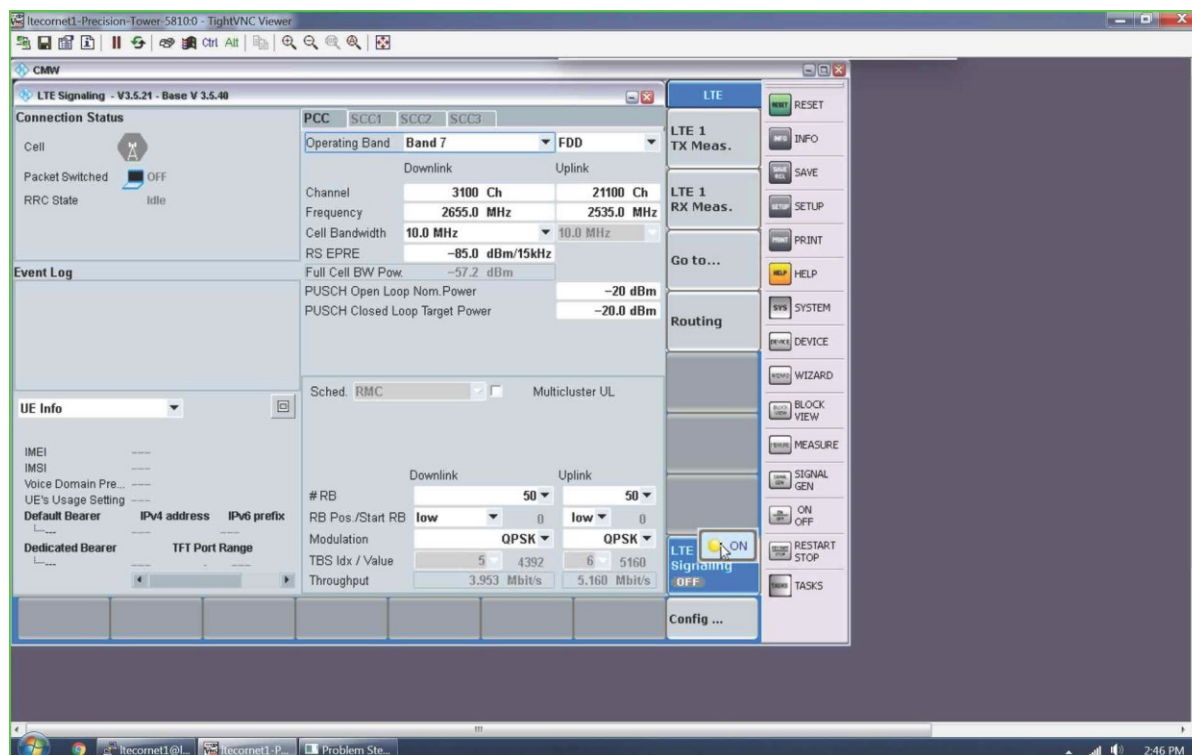


Figure 27: Turning the Signal Generator ON/OFF using the CMW500 interface.

6.3.4 UE

Two UEs have been used extensively for experimentation with the testbed, namely the Rogers AirCard 330U by Sierra Wireless, and the B593s router by Huawei. This section describes the basic operation and configuration of the same for use with the testbed. For more information on specific device, refer to the UE sub-section in the testbed document, and also to the respective devices' documentation.

UE interfaces have a lot of common features, and the points described here could be used for other manufacturer's devices as well. It is always a good idea to check these settings before using a device for the testbed, and resetting it to factory condition and starting configuration over if needed.

Using the Rogers AirCard 330U:

1. Check that a correct test-sim is inserted correctly into the UE. The USIM details would be needed for authentication on the network.
2. The Rogers UE has been tested with Windows machines. When the UE is first plugged into the computer's USB port, the driver installation menu launches automatically. Follow the on-screen instructions and the necessary drivers and the Rogers Connection Manager utility are installed.
3. Follow the path Options -> Network and verify that the all of the LTE frequency bands are selected for use.
4. Follow the path Options -> Profiles -> Rogers LTE -> Advanced -> TCP/IP settings and verify that parameters are configured correctly.

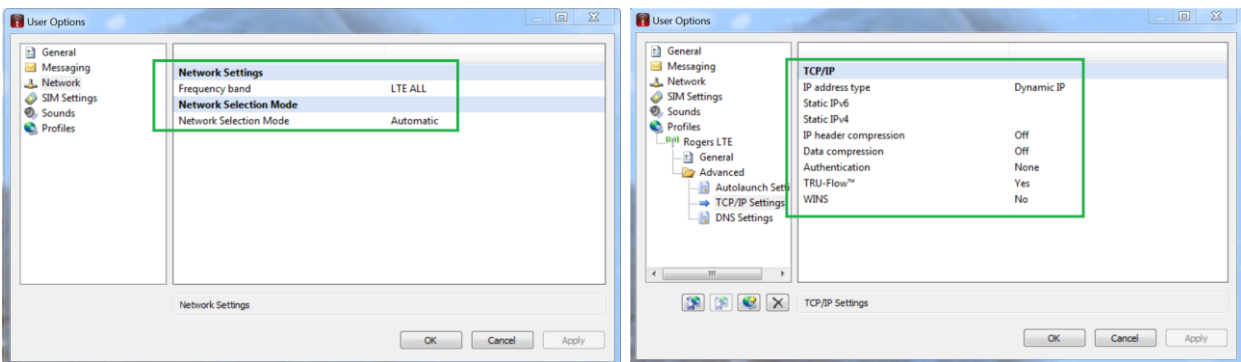


Figure 28a,b: Configuring the Rogers UE.

Using the Huawei B593s:

1. The Huawei B593s router does not require any drivers to be installed for its operation. Its internal page can be accessed using any internet browser on any platform by connecting over LAN on any one of the 4 LAN ports.
2. Check the device documentation for the path to the internal page as it may be different across different generations of the same device. For the current devices, it is located at:

`http://192.168.8.1/html/home.html`

3. The default login id is `admin` and the password is `admin` as well. It is a good practice to either leave the default login unchanged, or to make a note of the new login information if modifying the same.
4. For network settings, it is a good idea to have the router connect only to LTE networks, and turn on the option for Data Roaming.

6.3.5 RF Switch

The signal path can be routed using the RF Switches to change between the emulated and radiated modes respectively. Each of the switches can be accessed by bringing up the *http* page associated with its IP address to modify the switch position. Lookup tables for different combinations of the switches are given in Appendix J of this document.

6.3.6 iperf and jperf

The freeware software iPerf was used to measure the throughput of the link. iPerf is a network-testing tool generates data streams over both Transmission Control Protocol (TCP) and User Datagram Protocol (UDP), and has a client-server functionality to measure the amount of data transferred between the two ends [5]. One key difference between the two protocols is, TCP waits for acknowledgement after sending a large block of data, while UDP generally keeps sending data through assuming the receiver has received it. While both protocols could be used for the test, UDP was chosen for the measurements as it results in slight time savings during the measurement. Also, UDP reports higher throughput values than TCP, as the latter tends to control the data flow to avoid congestion, rather than trying to push the maximum amount of data through.

To maximize the data transfer over the link, parallel data streams were created. As the number of data streams increases, the computational power requirements of both the client and server computers increases. Hence, to strike a balance with the hardware in the setup, a maximum of 5 parallel streams, each with a maximum bandwidth of 1 GB/s were used to prevent any bottleneck due to data generation.

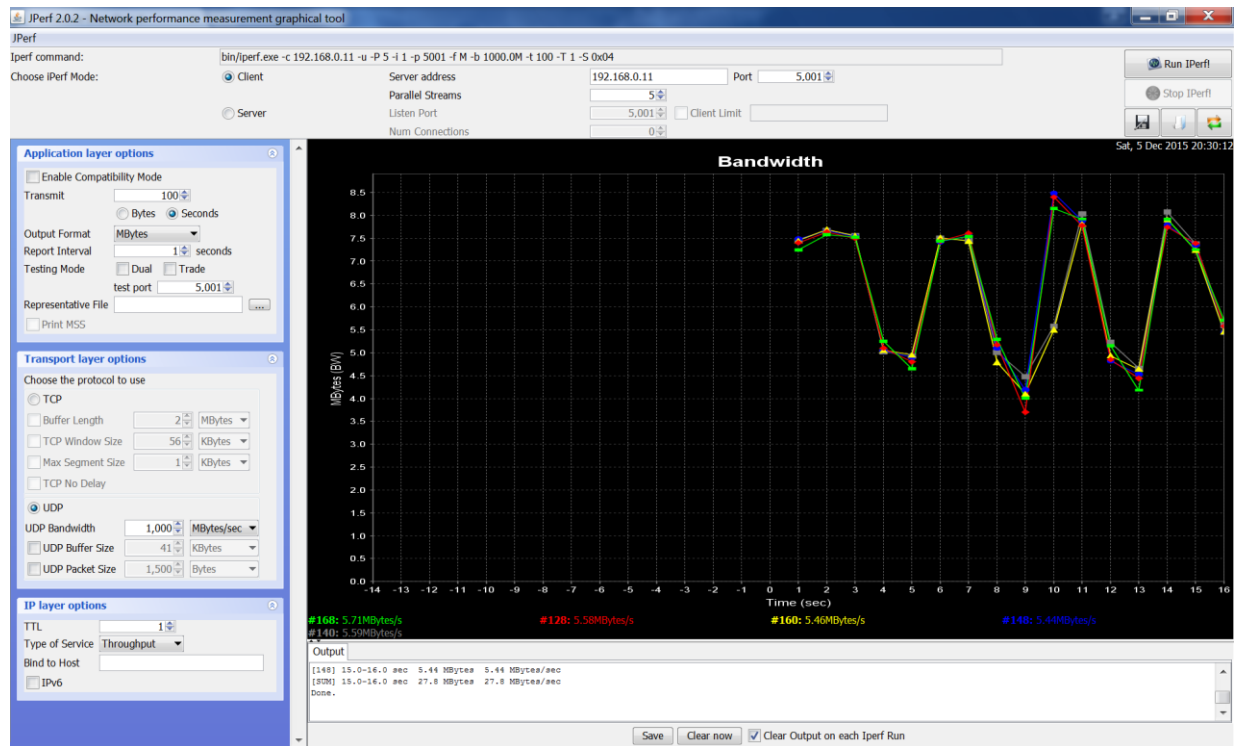


Figure 29: JPerf (a GUI interface for iPerf) reporting throughput in real-time.

The flow of actions for carrying out measurements was as follows:

- Initialize and start Amarisoft MME
- Initialize and start Amarisoft eNodeB
- Check and verify UE connection to network
- Get RSRP received at UE
- Initialize iPerf client at eNodeB, and iPerf server at UE
- Measure throughput for 100 seconds with 5 parallel data streams, while verifying UE connection
- Compute average throughput from these 100 data points for above RSRP

7. System Administration

The LTE-CORNET testbed can be administered remotely. User accounts can be setup for individual or a set of nodes. A few personal accounts have been created as well as generic student accounts that can be used to provide access to attendees of CORNET tutorials, among others. Only the system administrator account has root privileges.

Maintenance may occasionally require site visits.

Portable and mobile nodes, additional fixed node mounts, antennas, as well as other support equipment is located in Durham 439 and can be checked out for conducting experiments. The equipment is to be exclusively used for conducting related research or education or for the purpose of advancing the O-CORNET infrastructure and will be locked in drawers while not in use. Wireless@Virginia Tech will manage the equipment and maintain a log file with regular backups to keep track of the equipment as well as the experiments that are being conducted. The CORNET Web Site will serve as a portal for this.

8. Testbed Use in Research and Education

8.1 Education

The testbed has been used by students of the graduate Cellular Communication Systems and Software-Defined Radio classes at Virginia Tech. Students used the fixed and mobile nodes for experimenting with LTE signals and open-source SDR software libraries and frameworks. An example class project from the 2013 Software-Defined Radio class is described in continuation.

Fifth generation (5G) wireless networks are predicted to be optimized at each layer of the protocol stack to meet the necessary $1000\times$ capacity enhancement. At the physical layer, there is widespread research focus on alternate waveforms that have better characteristics than OFDM used in 4G. Some of the waveform contenders include Filter-bank Multicarrier (FBMC), Universal Filtered Multicarrier (UFMC), and Faster than Nyquist (FTN) [23]. We have taken a step forward in this direction by porting a Filtered Multi-Tone FBMC (FMT-FBMC) waveform on a Universal Software Radio Peripheral (USRP) using GNU Radio. This was part of an SDR class project at Virginia Tech in 2015. More precisely, the FMT-FBMC transceiver is implemented in GNU Radio [6] to demonstrate communication using four parallel 16-QAM symbol streams or subchannels. The software runs on PC2 and the RF signal through RFnest with 30 dB attenuation. Figure 30 illustrates the received constellation diagrams for the four symbols streams before equalization. The constellation is rotated with respect to the ideal constellation being the result of uncompensated phase shifts due to propagation delays.

This implementation can be extended to operate at full capacity using Staggered Multi-tone FBMC (ST-FBMC) at full-capacity [24].

Open source software toolboxes, such as GNURadio [6], srsLTE [4], and liquidDSP [25], can be used on our testbed to design and prototype new signal processing algorithms and protocols for the evolution of 4G LTE or new 5G waveforms.

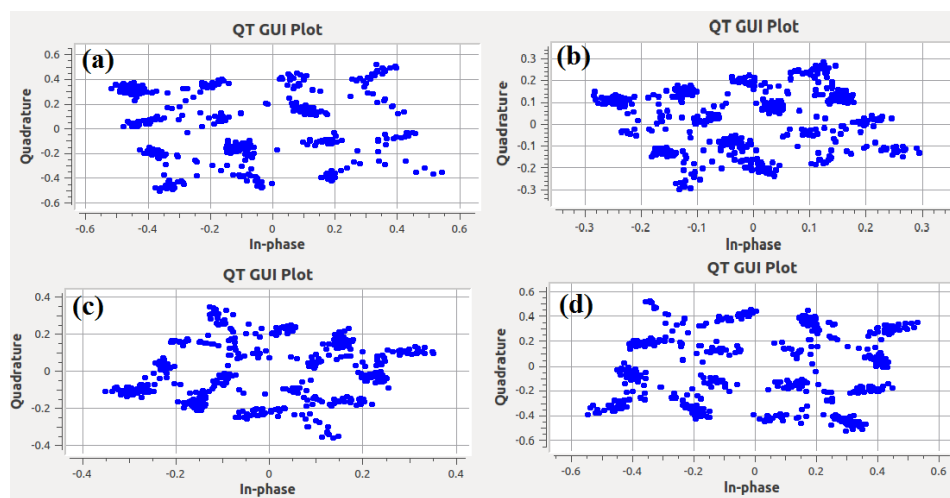


Figure 30: Constellation diagram of the four 16-QAM data streams of the FMT-FBMC waveform.

8.2 Research

8.2.1 LTE Evolution into Shared and Unlicensed Spectrum

Facing the need of $1000\times$ enhancement in capacity by 2020, the wireless research community is on the pursuit of technologies to bridge this gap. One of the ways this has been proposed to be implemented in the near future, is by extending LTE into the unlicensed and shared spectrum. One approach is aggregating bandwidth in shared spectrum as a secondary cell to the primary cell in licensed spectrum through the LTE-A feature *carrier aggregation* [22]. This technology is being termed as LTE-Unlicensed (LTE-U) or Licensed Assisted Access (LAA) and is currently standardized by the 3GPP, although other proposals for LTE-Unlicensed exist. It targets the 5 GHz band, which is used by WiFi and radar systems. LTE is also considered for deployment in the new shared bands, such as the new 3.5 GHz band and the AWS-3 bands in the US.

One of the challenges of operating LTE in unlicensed and shared spectrum is the ability to coexist with legacy systems in that band. Since LTE will be the secondary user system, it will need to back off whenever the primary or incumbent access (IA) user uses the band. There is some timeframe x within which the channel needs to be vacated. Ideally, within this timeframe, the LTE system should find another band and handoff all its users with an active session without disrupting or terminating the service. We define *interfering cell* as the cell that would interfere with the primary or incumbent access users and propose using handover as a mechanism for the secondary users to vacate to another band whenever primary or incumbent access users need access to the band. Here we discuss two mechanisms that we tested for multi-cell handovers using two (primary) cells at different center frequencies (EARFCNs) that are supported by the UEs:

1. Gradually lower the power of the interfering cell upon detection of a primary user such that there is a smooth transition of the UE from one cell to another.
2. Force the user to move out of the interfering cell by turning the cell off upon detection of the presence of primary users. This would result in cell reattachment and disrupts the active session.

In addition to initial cell deployments, we can rapidly deploy a new cell in a different band, and force the user to move into that cell or, handover the UE to the newly deployed cell gradually. Based on initial experiments, we are able to execute the entire process within one minute. Stricter channel vacation and UE handover or reattachment times are needed, which requires more research. We performed experiments on forced handovers, using our testbed. LTE100 was used to set up two FD-LTE cells in adjacent channels with a single B210 USRP: cell 0x01 (DL: 2680 MHz, UL: 2560 MHz) and cell 0x02 (DL: 2674.9 MHz, UL: 2544.9 MHz). Figure 31 shows the stages of forcing a user out of the interfering cell, which in this case is cell 0x01. Even though this experiment is carried out in LTE Band 7, it is representative of the scenarios that would occur in shared or unlicensed bands.

Instead of using two primary cells, we can use one primary cell and one or more secondary cells through the carrier aggregation feature of LTE-A, which is supported by Amarisoft's LTE100 eNB.

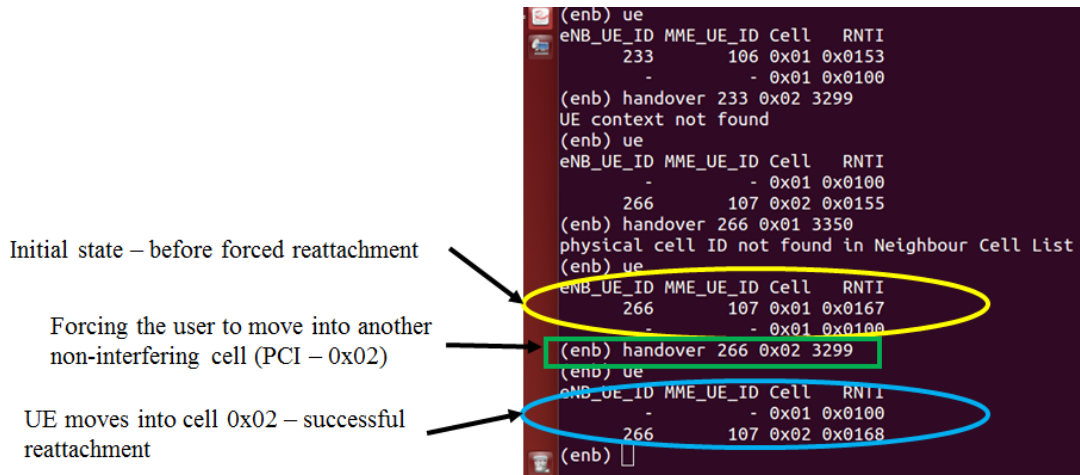


Figure 31: Snapshot showing the stages of forced handover with the forced handover feature of LTE100.

8.2.2 LTE for Mission-critical Networks

LTE has been used in the domain of public safety (FirstNet), and military communication networks in USA. Since commercialization of LTE has resulted in the public availability of standards documentation, adversaries with malicious intent could leverage this to target weak spots in the LTE protocol stack in order to enhance the potency of their attack.

We carried out several experiments to assess the impact of jamming and spoofing on LTE/LTE-A and proposed mitigation strategies to protect against the most efficient adversarial attacks that can cause Denial-of-Service (DoS). Figure 32 shows one of our experiment configurations using a combination of fixed and mobile testbed nodes. See [26], [27], and [29] for more information.

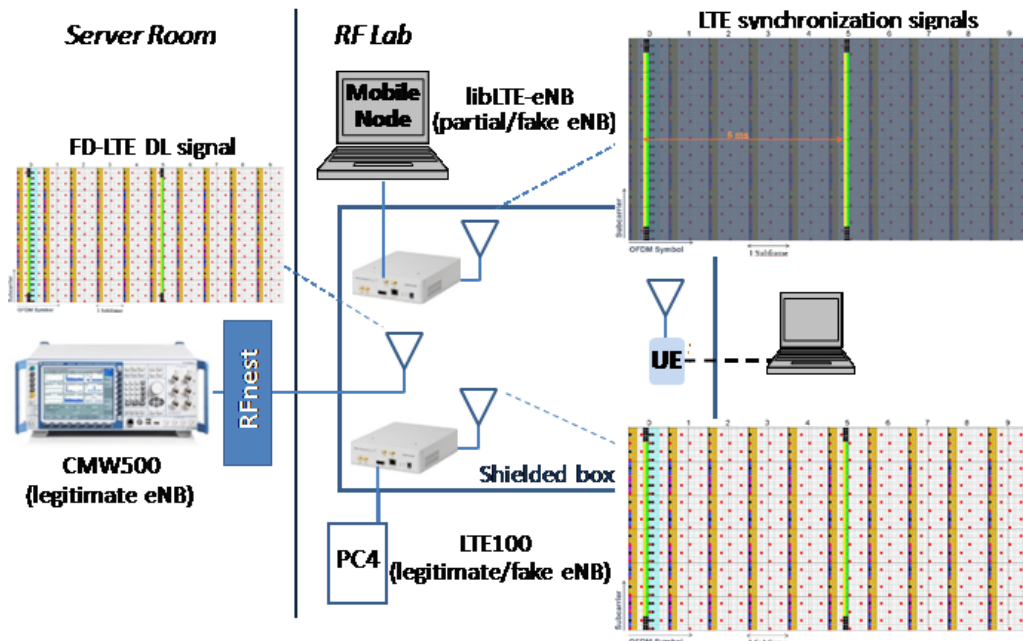


Figure. 32: Experiment setup for the LTE vulnerability analyses of [26] [27] [29].

9. Conclusions and Lessons Learned

The combined LTE-CORNET/COMWITS testbed has enabled research and education in 4G LTE and its evolution into shared spectrum. It supports experimental validation of theoretical research results. Students and researchers have used this testbed for education and experiments (see Section 8) and initial research results have been published in peer-reviewed journals and conference proceedings (see Appendix C).

The testbed will continue to enable research and education in emerging areas of communications with applications to commercial (4G, 5G), military, hospitals of the future, IoT, and many other systems. Some of the lessons learned are described below.

A. Computing power

The CPU load at the software eNodeB is proportional to the LTE bandwidth. Using a bandwidth greater than 10 MHz resulted in a large number of underflow/overflow errors when communicating with the USRP device due to not enough CPU time being available. Even at 10 MHz, care had to be taken while running additional software packages like iPerf to prevent these errors.

B. Heating of USRP

Since the USRP was operated at high data rates inside a shielded enclosure, the heat generated by the device would frequently lead to oscillator drift and frequent disconnection of the UE. Hence, it was necessary to stop and restart the eNodeB signalling before each measurement to prevent overheating.

C. UE Disconnection

Occasionally, the UE behaviour was erratic and it would refuse to latch onto the network. On other occasions, it would randomly disconnect from the network. This was initially suspected to be an issue with device authentication, and a number of test USIMs and IMSI combinations were attempted, but there was not much luck. Finally, the only reliable option to shake the UE out of its random behaviour was to do a full factory reset of its internal settings.

D. Throughput measurements

When LTE throughput is measured in uplink or downlink, separate RF paths are needed to provide separate attenuation on uplink and downlink to avoid disconnection of UEs because of weak downlink signals when measuring uplink throughput. Note that the LTE test equipment used has different output powers than regular LTE equipment. In particular, the SDR or CMW500 RF outputs can be significantly lower than the UE output power. Reference signal received power measured at the UE is accurately reported to the eNB. CQI and MCS are tightly correlated with each other. Monitoring MCS helps analyzing results, because there are standard tables that related MCS and transport block sizes [12]

E. MIMO measurements

During MIMO measurements it was observed that increasing the analog gains of the USRPs tend to cause frequent UE disconnections.

F. Performance of Cat. 3 UEs

When referring to 2x2 MIMO operation with Cat. 3 UEs, it is important to understand that they support only two layers of spatial multiplexing on the DL, but not on the UL. This means that with a Cat. 3 UE, the

maximum UL data rate that can be achieved is that as of the SISO case. Further, Cat. 3 UEs can achieve a maximum of 64 QAM only in DL (MCS 28) while they are limited to a maximum modulation scheme of 16QAM in the UL (MCS 20).

References

- [1] CORNET Web Site, <http://cornet.wireless.vt.edu>
- [2] Tektronix H500/SA2500 Datasheet, <http://www.tek.com/sites/tek.com/files/media/media/resources/H500-SA2500-Spectrum-Analyzer-Datasheet-1.pdf>
- [3] PEAR™ S4935i Pigtail Broadband In-Building Antenna Datasheet, <http://www.galtronics.com/wp-content/uploads/2015/02/Galtronics-PEAR-S4935i-Pigtail-Datasheet.pdf>
- [4] srsLTE - Open-Source LTE, <https://github.com/srsLTE/srsLTE>
- [5] The OpenAirInterface Software Alliance (OSA), <http://www.openairinterface.org/>
- [6] Install GNU Radio, <http://gnuradio.org/redmine/projects/gnuradio/wiki/InstallingGRFromSource>
- [7] PuTTY homepage, <http://www.putty.org/>
- [8] TightVNC, <http://tightvnc.com/download.php>
- [9] iPerf homepage, <https://iperf.fr/>
- [10] JPerf download page, <https://sourceforge.net/projects/jperf/>
- [11] Technical specifications for Sierra Wireless AirCard® 330U LTE Mobile Broadband Modem, <http://www.rogers.com/cms/images/en/Wireless/CellPhoneDetail/Support/Sierra-Wireless-AirCard330Uen.pdf>
- [12] Technical Specification, LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer procedures (3GPP TS 36.213 version 12.4.0 Release 12)
- [13] *LTE Physical Layer Overview*, White Paper, http://rfmw.em.keysight.com/wireless/helpfiles/89600B/WebHelp/Subsystems/lte/content/lte_overview.htm
- [14] Sesia, Stefania, Issam Toufik, and Matthew Baker. *LTE--the UMTS long term evolution: from theory to practice*, Wiley, Chichester, West Sussex, U.K; Hoboken, N.J, 2011.
- [15] Huawei E8278, “User guide.”
- [16] Product details, <http://www.ebay.com/bhp/huawei-4g-antenna>
- [17] LTE Transmission Modes and Beamforming, White Paper, Rohde & Schwarz. https://cdn.rohde-schwarz.com/pws/dl_downloads/dl_application/application_notes/1ma186/1MA186_2e_LTE_TMs_and_beamforming.pdf
- [18] User Equipment Category, http://niviuk.free.fr/ue_category.php
- [19] UE Categories, <https://en.wikipedia.org/wiki/E-UTRA>
- [20] Benny Bing, *Broadband wireless multimedia networks*, Wiley, a John Wiley & Sons Inc., Publication, Hoboken, New Jersey, 2013.
- [21] *LTE-Advanced Physical Layer*, Presentation Material, ftp://www.3gpp.org/workshop/2009-12-17_ITU-R_IMT-Adv_eval/docs/pdf/REV-090003-r1.pdf
- [22] R. Zhang, M. Wang, L. X. Cai, Z. Zheng, X. Shen and L. L. Xie, “LTE unlicensed: the future of spectrum aggregation for cellular networks,” in *IEEE Wireless Communications*, vol. 22, no. 3, pp. 150-159, June 2015.
- [23] P. Banelli, S. Buzzi, G. Colavolpe, A. Modenini, F. Rusek and A. Ugolini, “Modulation Formats and Waveforms for 5G Networks: Who Will Be the Heir of OFDM? – An overview of alternative modulation schemes for improved spectral efficiency,” *IEEE Signal Processing Magazine*, vol. 31, no. 6, pp. 80-93, Nov. 2014.
- [24] M. Bellanger, “FBMC physical layer: a primer”, PHYSDYAS, 2010, URL: http://www.ict-phydyas.org/teamspace/internal-folder/FBMC-Primer_06-2010.pdf
- [25] liquidsdr.org - Making Software Radio Portable Homepage, <http://liquidsdr.org/>
- [26] M. Lichtman, R. P. Jover, M. Labib, R. M. Rao, V. Marojevic, J. H. Reed, “LTE/LTE-A Jamming, Spoofing and Sniffing: Threat Assessment and Mitigation,” *IEEE Commun. Mag.*, vol. 54, no. 4, pp. 2-9, April 2016.

- [27] M. Labib, V. Marojevic, J. Reed, “Analyzing and enhancing the resilience of LTE/LTE-A,” *Proc. IEEE Conf. Standards for Communications and Networking (CSCN)*, Tokyo, Japan, 28-30 Oct. 2015.
- [28] FCC Experimental license for Virginia Tech’s O-CORNET Testbed, <https://apps.fcc.gov/els/GetAtt.html?id=154653&x=>
- [29] M. Labib, V. Marojevic, J.H. Reed, A.I. Zaghloul, “Enhancing the robustness of LTE systems: analysis and evolution of the cell selection process,” *IEEE Commun. Mag.*, *accepted Aug. 2016, to be published*.
- [30] Sierra Wireless AirCard 330U, “Quick start guide,” <https://www.sierrawireless.com/>
- [31] Huawei E3276 4G LTE Mobile Internet Key, “User guide,” Version: V100R001_01 Part Number: 31010NWB.
- [32] Huawei Technologies Co., Ltd, “Welcome to the LTE CPE! - Online help.”

Appendix A

Modulation and Coding Schemes in LTE

Depending on the channel conditions reported back by the UE, the eNodeB adapts the modulation and coding scheme (MCS) on the DL to maximize the data rate to the UE. The eNodeB can select among QPSK, 16QAM and 64QAM modulation schemes and a variety of code rates, with the optimal switching points between the combinations depending on a number of factors including required quality of service and cell throughput. On the UL, the eNodeB can estimate the channel conditions on its own by channel sounding, and carry out the link adaption accordingly. The eNodeB can choose between QPSK and 16QAM with the highest category of UEs using 64QAM [A.1].

Tables A.1 and A.2 are adapted from 3GPP TS 36.213 [A.2] and show the mapping of MCS Index (I_{MCS}) to Transport Block Size (TBS) Index (I_{TBS}) on the DL and UL respectively. For both the DL and UL, the MCS takes one of 32 possible values from 0 to 31, with higher values indicating use of higher order modulation schemes and lower coding overhead. The MCS index determines the TBS Index (I_{TBS}) and ultimately the throughput on the link; with higher TBS indexes resulting into bigger TB sizes and higher throughput. Since MCS indexes 29-31 are reserved for future use in both UL and DL, a MCS of 28 gives the highest throughput. For the UL, the highest non-64QAM MCS is 20.

The modulation order (Q_m) indicates the number of bits mapped on to a symbol, and it takes values of 2, 4 and 6 corresponding to the modulation schemes of QPSK, 16QAM and 64QAM respectively. Upon comparing tables A.1 and A.2 it can be observed that a given MCS index maps to a higher modulation order on the DL as compared to the mapping of the same MCS index on the UL side.

Table A.1. Modulation and TBS index table for PDSCH adapted from Table 7.1.7.1-1 [A.2].

MCS Index I_{MCS}	Modulation Order Q_m	TBS Index I_{TBS}	MCS Index I_{MCS}	Modulation Order Q_m	TBS Index I_{TBS}	MCS Index I_{MCS}	Modulation Order Q_m	TBS Index I_{TBS}
0	2	0	11	4	10	22	6	20
1	2	1	12	4	11	23	6	21
2	2	2	13	4	12	24	6	22
3	2	3	14	4	13	25	6	23
4	2	4	15	4	14	26	6	24
5	2	5	16	4	15	27	6	25
6	2	6	17	6	15	28	6	26
7	2	7	18	6	16	29	2	reserved
8	2	8	19	6	17	30	4	
9	2	9	20	6	18	31	6	
10	4	9	21	6	19	---		

Table A.2. Modulation and TBS index table for PUSCH adapted from Table 8.6.1-1 [A.2].

MCS Index <i>I_{MCS}</i>	Modulation Order <i>Q_m</i>	TBS Index <i>I_{TBS}</i>	MCS Index <i>I_{MCS}</i>	Modulation Order <i>Q_m</i>	TBS Index <i>I_{TBS}</i>	MCS Index <i>I_{MCS}</i>	Modulation Order <i>Q_m</i>	TBS Index <i>I_{TBS}</i>
0	2	0	11	4	10	22	6	20
1	2	1	12	4	11	23	6	21
2	2	2	13	4	12	24	6	22
3	2	3	14	4	13	25	6	23
4	2	4	15	4	14	26	6	24
5	2	5	16	4	15	27	6	25
6	2	6	17	4	16	28	6	26
7	2	7	18	4	17	29	reserved	
8	2	8	19	4	18	30		
9	2	9	20	4	19	31		
10	2	10	21	6	19	---		

References

- [A.1] Sesia, Stefania, Issam Toufik, and Matthew Baker. *LTE--the UMTS long term evolution: from theory to practice*, Wiley, Chichester, West Sussex, U.K; Hoboken, N.J., 2011.
- [A.2] Technical Specification, LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer procedures (3GPP TS 36.213 version 12.4.0 Release 12).

Appendix B

Theoretical LTE Peak Throughput

One LTE frame has a duration of 10 ms and consists of ten subframes of 1 ms duration. The subframe can be further divided into two slots of 0.5 ms. One slot carries 7 OFDM symbols with the normal cyclic prefix (CP), and 6 OFDM symbols when the extended CP is used. A Resource Element (RE) carries a modulation symbol or its equivalent using one subcarrier for a duration of one OFDM symbol. A Resource Block (RB) comprises of 84 REs for the case of normal CP length and 72 REs when the extended CP is used [B.1].

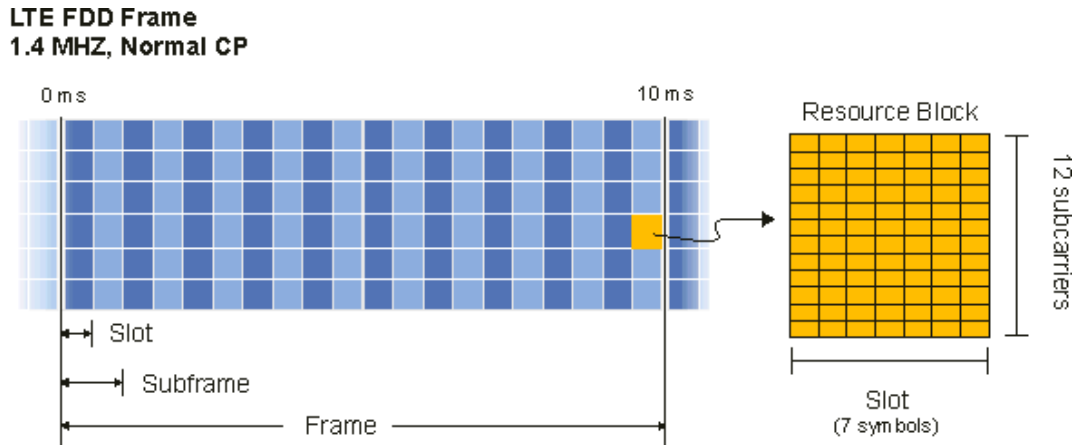


Figure B.1: Illustration of a UL/DL LTE frame [B.2].

Given a particular LTE configuration, bandwidth and MCS index in use, it is possible to estimate the expected data rates on DL and UL. This section presents two approaches for the same - an approximate approach that uses rule-of-thumb calculations, and a more accurate method that uses the 3GPP technical specifications data.

B.1 Using rule-of-thumb calculations

The peak data throughputs on the DL and UL can be computed intuitively using the knowledge of the LTE physical layer parameters. Consider a 5 MHz SISO FD-LTE system. The number of REs in one frame can be calculated as

$$\text{RE_per_subframe_5MHz} = 25 \text{ RBs} \times 12 \text{ subcarriers} \times 7 \text{ OFDM symbols} \times 2 \text{ slots} = 4200 \text{ REs/ms.}$$

Since the highest modulated on the DL is 64-QAM, there are 6 bits modulated per 64-QAM symbol, i.e. 6 bits/symbol. Assuming no coding overhead, this gives a total data rate of

$$\text{Max_throughput_5MHz_64QAM} = 6 \text{ bits/symbol} \times 4200 \text{ REs/ms} = 25.2 \text{ Mb/s.}$$

A rule of thumb suggests assuming a signalling overhead of 25% for the LTE physical control channels. Hence, the resulting peak data rate for user data for the 5 MHz system and 64-QAM modulation becomes 18.9 Mb/s. For 2x2 MIMO/spatial multiplexing system, the peak data rate can be estimated as $18.9 \text{ Mb/s} \times 2 = 37.8 \text{ Mb/s}$.

For the UL, instead of 64-QAM (6 bits per symbol), we have a maximum modulation scheme of 16-QAM (4 bits per symbol) for the early LTE UEs (up to Cat. 4). The theoretical peak data rate for user data then reduces to $\frac{2}{3} \times 18.9 \text{ Mb/s} = 12.6 \text{ Mb/s}$ and 25.2 Mb/s for 2x2 MIMO.

Table B.1 summarizes the peak DL and UL data rates using this method.

Table B.1. Theoretical peak data rates in LTE, assuming a 25% signalling overhead

Configuration	LTE Bandwidths					
	5 MHz		10 MHz		20 MHz	
	DL ¹	UL ¹	DL ¹	UL ¹	DL ¹	UL ¹
SISO	18.9 Mb/s	12.6 Mb/s	37.8 Mb/s	25.2 Mb/s	75.6 Mb/s	50.4 Mb/s
2x2 MIMO	37.8 Mb/s	25.2 Mb/s	75.6 Mb/s	50.4 Mb/s	151.2 Mb/s	100.8 Mb/s

¹ UL uses 16-QAM, DL uses 64-QAM modulation. This table assumes that 2x2 spatial multiplexing is supported on both the DL and UL.

B.2 Using 3GPP specs

The 3GPP Technical Specifications can be used to accurately compute the number of Transport Blocks and the associated data rate on DL and UL respectively. The procedure for computing the DL data rate is as follows:

- Using the Modulation and Coding Scheme (I_{MCS}) index, compute the Modulation Order (Q_m) and TBS Index (I_{TBS}) parameters using Table 7.1.7.1-1: Modulation and TBS index table for PDSCH from Page 60 of 3GPP TS 36.213 version 12.4.0 (Release 12), for instance [B.3].
- The Transport Block Size (TBS) Index (I_{TBS}) along with the number of physical layer resource blocks (N_{PRB}) are used to determine the TBS. ($N_{PRB} = 25, 50, 100$ for 5, 10, 20 MHz.)
- For a SISO case, where $1 \leq N_{PRB} \leq 100$, the TBS is given by the (I_{TBS}, N_{PRB}) entry of Table 7.1.7.2.1-1: TBS table (dimension 34×110) on Page 62 of [B.3].
- For a 2x2 MIMO case, where the Transport Blocks are mapped to two-layer Spatial Multiplexing, the TBS is read off differently from the table:

- For $1 \leq N_{PRB} \leq 55$, the TBS is given by the $(I_{TBS}, 2 \times N_{PRB})$ entry of Table 7.1.7.2.1-1: TBS table (dimension 34×110) on Page 62 of [B.3].
- For $56 \leq N_{PRB} \leq 110$, the the (I_{TBS}, N_{PRB}) entry of Table 7.1.7.2.1-1: TBS table (dimension 34×110) on Page 62 of [B.3] gives the baseline TBS_L1.
- The baseline TBS_L1 is translated into TBS_L2 using the mapping rule given in Table 7.1.7.2.2-1: One-layer to two-layer TBS translation table on Page 69 of [B.3]. TBS_L2 is the TBS for this case.
- TBS has units of bits. A new transport block is processed every a transmission time interval (TTI) of 1 ms. Thus, the data rate can be translated to Mb/s as $TBS \times 10^{-3}$ [Mb/s].

The procedure for computing the data rate on the UL is similar to the above method, and uses the equivalent PUSCH tables from the same document [B.3]. First, the Modulation Order (Q_m) and TBS Index (I_{TBS}) parameters are obtained using Table 8.6.1-1: Modulation, TBS index and redundancy version table for PUSCH from Page 146 of 3GPP TS 36.213 version 12.4.0 Release 12 [B.3]. Next, using this value of TBS Index, the above procedure is repeated to get the TBS and throughput on the UL.

The peak data rates for the SISO and 2x2 MIMO configurations have been computed for the 5, 10 and 20 MHz LTE systems and summarized in Tables B.2 - B.5 respectively. As can be observed, the assumption of 25% signalling overhead and no coding when computing peak throughput by the the rule-of-thumb holds fairly well for each of these configurations, and the computed rates are very close to those computed using the 3GPP specs. For the 5 MHz SISO configuration, peak data rate is found to be 18.9 Mb/s by the rule-of-thumb calculations, and 18.336 Mb/s by using the specifications.

Table B.2. Summary of peak DL data rates according to 3GPP specs and computed for SISO.

LTE Bandwidth	Computing Modulation order using Table 7.1.7.1-1: Modulation and TBS index table for PDSCH from [B.3]			Computing Transport Block Size using Table 7.1.7.2.1-1: Transport block size table from [B.3]			Theoretical Peak Throughput according to 3GPP specs [Mb/s]	Computed Peak Throughput by rule-of-thumb [Table B.1] [Mb/s]
	MCS Index I_{MCS}	Modulation Order Q_m	TBS Index I_{TBS}	TBS Index I_{TBS}	N_{PRB}	TBS		
5 MHz	27	6	25	25	25	15840	15.840	N/A
5 MHz	28	6	26	26	25	18336	18.336	18.9
10 MHz	28	6	26	26	50	36696	36.696	37.8
20 MHz	28	6	26	26	100	75376	75.376	75.6

Table B.3. Summary of peak UL data rates according to 3GPP specs and computed for SISO.

LTE Bandwidth	Computing Modulation order using Table 8.6.1-1: Modulation, TBS index and redundancy version table for PUSCH from [B.3]			Computing Transport Block Size using Table 7.1.7.2.1-1: Transport block size table from [B.3]			Theoretical Peak Throughput according to 3GPP specs [Mb/s]	Computed Peak Throughput by rule-of-thumb [Table B.1] [Mb/s]
	I_{MCS}	Q_m	I_{TBS}	I_{TBS}	N_{PRB}	TBS		
5 MHz	20	4	19	19	25	10680	10.680	12.6
5 MHz	28	6	26	26	25	18336	18.336	18.9
10 MHz	20	4	19	19	50	21384	21.384	25.2
10 MHz	28	6	26	26	50	36696	36.696	37.8
20 MHz	20	4	19	19	100	43816	43.816	50.4
20 MHz	28	6	26	26	100	75376	75.376	75.6

Note that Cat. 3 UEs do not support 64QAM on the UL. Hence we included the MCS of 20, being the highest-rate 16QAM UL transmission mode. The lower MCS values have been observed during some measurements, and included for reference.

Table B.4. Summary of peak DL data rates according to 3GPP specs and computed for 2x2 MIMO.

LTE Bandwidth h	Computing Modulation order using Table 7.1.7.1-1: Modulation and TBS index table for PDSCH from [B.3]			Computing Transport Block Size using					Theoretical Peak Throughput according to 3GPP specs [Mb/s]	Computed Peak Throughput by rule-of- thumb [Table B.1] [Mb/s]
				Table 7.1.7.2.1-1: Transport block size table from [B.3]			Table 7.1.7.2.2-1: One-layer to two- layer TBS translation table from [B.3]			
	I_{MCS}	Q_m	I_{TBS}	I_{TBS}	N_{PRB}	TBS	TBS_L1	TBS_L2		
5 MHz	27	6	25	25	25	31704	N/A		31.704	N/A
5 MHz	28	6	26	26	25	36696			36.696	37.8
10 MHz	28	6	26	26	50	75376			75.376	75.6
20 MHz	28	6	26	26	100	75376	75376	149976	149.976 ¹	151.2 ¹

¹ Theoretical peak throughput for Cat. 3 UEs is 102 Mb/s [B.4].

Table B.5. Summary of peak data rates according to 3GPP specs for two-layer spatial multiplexing in UL. Note that this is not valid for Cat 3 UEs since spatial multiplexing is not supported on the UL--Table B.3 applies instead.

LTE Bandwidth	Computing Modulation order using Table 8.6.1-1: Modulation, TBS index and redundancy version table for PUSCH from [B.3]			Computing Transport Block Size using					Theoretical Peak Throughput according to 3GPP specs [Mb/s]	Computed Peak Throughput by rule-of- thumb [Table B.1 [Mb/s]]
				Table 7.1.7.2.1-1: Transport block size table from [B.3]			Table 7.1.7.2.2-1: One-layer to two- layer TBS translation table from [B.3]			
	I_{MCS}	Q_m	I_{TBS}	I_{TBS}	N_{PRB}	TBS	TBS_L1	TBS_L2		
5 MHz	28	6	26	26	25	36696	Not applicable		36.696	37.8
10 MHz	28	6	26	26	50	75376			75.376	75.6
20 MHz	28	6	26	26	100	75376	75376	149776	149.776	151.2

References

- [B.1] Sesia, Stefania, Issam Toufik, and Matthew Baker. *LTE--the UMTS long term evolution: from theory to practice*, Wiley, Chichester, West Sussex, U.K.; Hoboken, N.J., 2011.
- [B.2] *LTE Physical Layer Overview*, White Paper,
http://rfmw.em.keysight.com/wireless/helpfiles/89600B/WebHelp/Subsystems/lte/content/lte_overview.htm.
- [B.3] Technical Specification, LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer procedures (3GPP TS 36.213 version 12.4.0 Release 12).
- [B.4] UE Categories, <https://en.wikipedia.org/wiki/E-UTRA>

Appendix C

Transmission Modes in LTE

MIMO technology and beamforming forms an integral part of the 3GPP LTE standard. The UE is required to be able to spatially multiplex two spatial streams in the downlink (DL). The UE may have additional antennas to support receive diversity in the DL. At the eNodeB, the baseline configuration uses two transmit antennas, at the UE the baseline configuration uses two receive and one transmit antenna [C.1].

LTE Release 12 provides for 10 Transmission Modes on the DL, and 2 Transmission Modes in the uplink (UL). Tables C.1 and C.2 summarize these modes. Amarisoft LTE100 supports all the 10 DL Transmission Modes and we have conducted tests in the cabled and radiated mode for TM3 with Cat 3 UEs. Cat 3 UEs support two layers of spatial multiplexing on the DL, but only a single layer or spatial stream on the UL. Thus, their peak UL data rate is same as that for the SISO UL case.

Table C.1. DL Transmission modes in LTE Release 12 [C.2].

Transmission Mode	Description	Comments
1	Single Transmit Antenna	single antenna port port 0
2	Transmit diversity	2 or 4 antennas ports 0,1 (...3)
3	Open loop spatial multiplexing with cyclic delay diversity (CDD)	2 or 4 antennas ports 0,1 (...3)
4	Closed loop spatial multiplexing	2 or 4 antennas ports 0,1 (...3)
5	Multi-user MIMO	2 or 4 antennas ports 0,1 (...3)
6	Closed loop spatial multiplexing using a single transmission layer	1 layer (rank 1), 2 or 4 antennas ports 0,1 (...3)
7	Beamforming	single antenna port, port 5 (virtual antenna port, actual antenna configuration depends on implementation)
8	Dual-layer beamforming	dual-layer transmission, antenna ports 7 and 8
9	8 layer transmission	Up to 8 layers, antenna ports 7 - 14
10	8 layer transmission	Up to 8 layers, antenna ports 7 - 14

Table C.2. UL Transmission modes in LTE Release 12 [C.2].

Transmission Mode	Description	Comments
1	Single Transmit Antenna	single antenna port (port 10)
2 ¹	Closed-loop spatial multiplexing	2 or 4 antennas (ports 20 and 21) (ports 40,41,42,43)

¹ Not supported by Cat 3 UEs.

References

- [C.1] Bing, Benny. *Broadband wireless multimedia networks*, Wiley, a John Wiley & Sons Inc., Publication, Hoboken, New Jersey, 2013;2012;.
- [C.2] LTE Transmission Modes and Beamforming, White Paper, Rohde & Schwarz.
https://cdn.rohde-schwarz.com/pws/dl_downloads/dl_application/application_notes/1ma186/1MA186_2e_LTE_TMs_and_beamforming.pdf.

Appendix D

UE Categories in LTE

The Category of the User Equipment (UE) defines its downlink and uplink capabilities, and allows the eNodeB to communicate effectively with it. Table D1 summarizes the five UE categories defined as per 3GPP TS 36.306 for LTE Release 8 based on the maximum peak data rates and MIMO capabilities of the device.

Category 3 UEs support upto 2 layers of DL MIMO and peak DL data rates of 102 Mbits/sec, while on the UL they do not support MIMO and have peak UL data rates of 51 Mbits/sec. The UL on Cat 3 UEs is limited to only one layer and 16QAM, while on the DL they can operate at 64 QAM and up to two layers of MIMO [D.1].

Table D1. UE Categories in LTE Release 8 as per 3GPP TS 36.306 [D.2].

UE Category	Maximum no. of DL MIMO Layers	Maximum L1 Data Rate on DL [Mb/s]	Maximum L1 Data Rate on UL [Mb/s]	64 QAM in UL
Category 1	1	10.3	5.2	No
Category 2	2	51.0	25.5	No
Category 3	2	102.0	51.0	No
Category 4	2	150.8	51.0	No
Category 5	4	299.6	75.4	Yes

Subsequent LTE Releases have added more categories, with Release 13 introducing Category 17 for the DL, supporting DL peak data rates of 25 Gbits/s with 8 MIMO DL layers and 256 QAM [D.3].

References

- [D.1] Bing, Benny. *Broadband wireless multimedia networks*, Wiley, a John Wiley & Sons Inc., Publication, Hoboken, New Jersey, 2013;2012;.
- [D.2] User Equipment Category, http://niviuk.free.fr/ue_category.php.
- [D.3] *LTE-Advanced Physical Layer*, Presentation Material, ftp://www.3gpp.org/workshop/2009-12-17_ITU-R_IMT-Adv_eval/docs/pdf/REV-090003-r1.pdf.

Appendix E

Initial Measurements for 2x2 LTE-MIMO: Cabled Mode

In order to verify the hardware capabilities of the testbed, and to serve as a proof-of-concept for 2x2 LTE MIMO operation, three hardware configurations have been tested: direct cabling between eNodeB and UE antennas, using RFnest channel emulator, and over-the-air (OTA) transmissions. For each case, the link performance is evaluated by comparing the measured throughputs against the expected theoretical throughput values computed in Appendix B.

This section describes the testing process and results from the trials carried out using a cabled setup.

E.1 Test setup

The block diagram for the measurement setup is as shown in Figure E.1. The eNodeB is emulated on a mobile workstation connected to the B210 USRP via USB 3.0. For this we use Amarisoft LTE100 v2016-23-06 and USRP Hardware Driver (UHD) version v003.008.004. The Rogers AirCard 330U is chosen for the UE. The Tx/Rx ports of the USRP are directly cabled with low-loss cables to the two antenna terminals of the UE as shown in Figure E.1 to emulate two ideal, independent channels between the transmit and receive antennas.

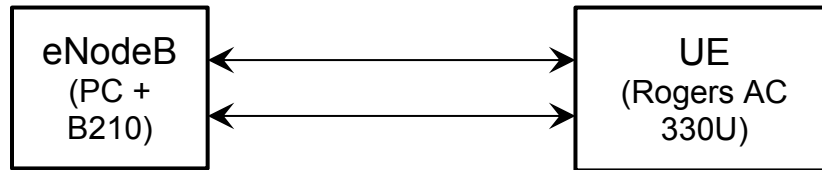


Figure E.1: Cabled mode setup for emulating two ideal channels between Tx and Rx antennas for 2x2 MIMO measurements.

Since the attenuation introduced by the cables is ~ 1 dB at the frequency of operation, the signal experiences minimal attenuation along the channel in this setup. Thus, in order to prevent saturation of the receiver chain, it is necessary to adjust the analog gains of the USRP RF front end using the '*tx_gain*' and '*rx_gain*' parameters of Amarisoft eNodeB. Starting initially with a low value of the gain parameter, the values were adjusted until the Channel Quality Indicator (CQI) reported by the UE was found to be maximum (15), corresponding to a reference signal received power (RSRP) of -83 dBm at 5 MHz LTE system bandwidth. The analog gains on the USRP were found to be fairly consistent and hence, once calibrated, the same values of gains were used for the other cases of 10 and 20 MHz LTE modes for stable operation. For higher transmit gain values, we observed UE disconnections.

Tests have been carried out in 3GPP FD-LTE Band 7 with a downlink frequency of 2680 MHz and uplink frequency of 2560 MHz for LTE bandwidths of 5 MHz, 10 MHz and 20 MHz respectively.

E.2 Test methodology

For data throughput measurement and verification we capture the data transfer count in the UE's Connection Manager software interface and the total data transferred as reported by the '*ifconfig*' command in Linux. iPerf is used to create data traffic and the total data transferred across the link observed for a given duration (100 s) to compute the average throughput. 100 seconds were chosen as it is sufficiently large when compared to the radio frame of 10 ms and the transmission time interval (TTI) of 1 ms, which is the base unit for resource allocation.

E.3 Test procedure

The MME on an emulated core network is launched first on the eNodeB-side PC, followed by launching the eNodeB. The UE connection is verified and the RSRP and RSRQ values reported.

For the downlink measurements, the iPerf server is launched on the computer connected to the UE, and the iPerf client running on the computer with the eNodeB connects to the iPerf server. Similarly, for the uplink measurements, the iPerf server is launched on the eNodeB side and the iPerf client running on the UE side connects with it. Throughput measurements are carried out for multiple iterations each of 100 seconds, using 20 parallel streams of UDP traffic with a maximum throughput of 100 Mbps. The command line parameters for the two cases are shown in Table E.1. The computer with the eNodeB can be identified by its IP address of 192.168.3.1, and the computer on the UE side is assigned an IP address of 192.168.3.1.

Table E.1. Command line parameters for iPerf measurements.

Measured Link	Computer on eNodeB side	Computer on UE side
Downlink (eNB to UE)	<code>iperf -c 192.168.3.2 -p 5001 -u -t 100 -P 20 -b 100M</code>	<code>iperf -s -u P 20 -i 10 -p 5001 -f m</code>
Uplink (UE to eNB)	<code>iperf -s -u P 20 -i 10 -p 5001 -f m</code>	<code>iperf -c 192.168.3.1 -p 5001 -u -t 100 -P 20 -b 100M</code>

The data transferred in 100 s is captured and the average measured calculated.

E.3 Results

For each of the cases, it is found that the once iPerf client is launched, the throughput ramps up and it takes a small time to reach the maximum rate. After the initial ramp, the throughput remains fairly consistent until the end of the data transfer, when it gradually drops to the minimum value. This behavior is expected as the UE buffer data streams and requests resources to the eNodeB based on the buffer status. Figure E.2 shows a screenshot of the eNodeB trace that highlights this process. The performance is calculated and reported about once per second. The left half of the log indicates the parameter values on the DL, while the right half corresponds to the UL. We see that the DL data rate is initial 2.39 kbps and later stabilizes at 31.1 Mbps.

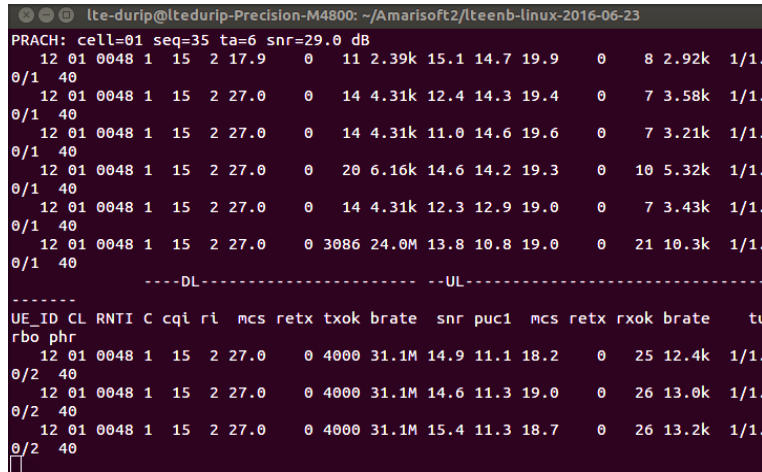


Figure E.2: Amarisoft eNodeB's MAC trace highlighting throughput ramping up during the 5 MHz DL measurement trial.

Figures E.3 to E.5 show the Amarisoft eNodeB's MAC trace during the measurements for 5, 10 and 20 MHz BW respectively. The throughput as indicated by the 'brat' column in the log shows a fairly consistent value during the measurement, after the initial ramp-up phase. Other parameters during the measurements such as the Rank Indicator (RI), CQI and MCS can also be observed.

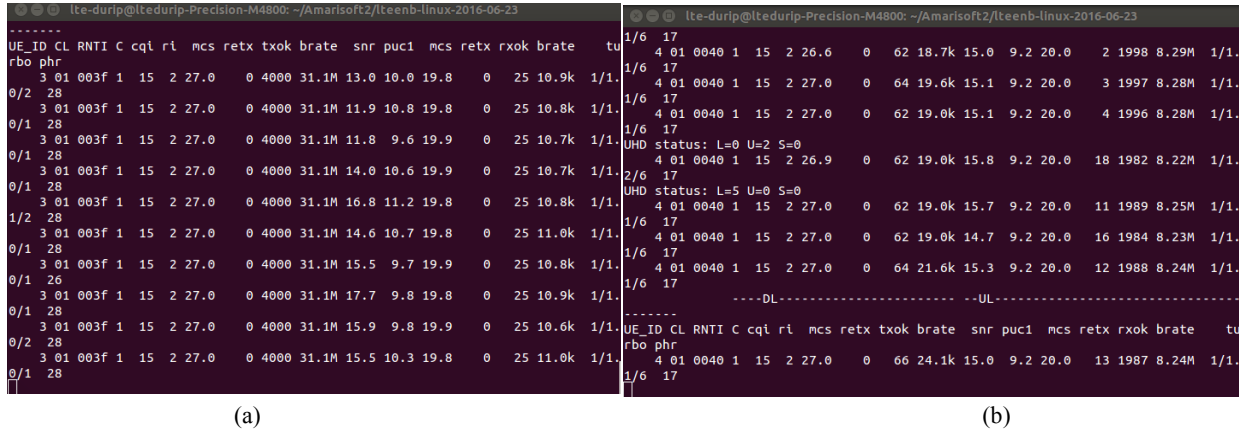


Figure E.3: Amarisoft eNodeB's MAC trace for (a) DL and (b) UL during measurement with 5 MHz BW and 2x2 MIMO.

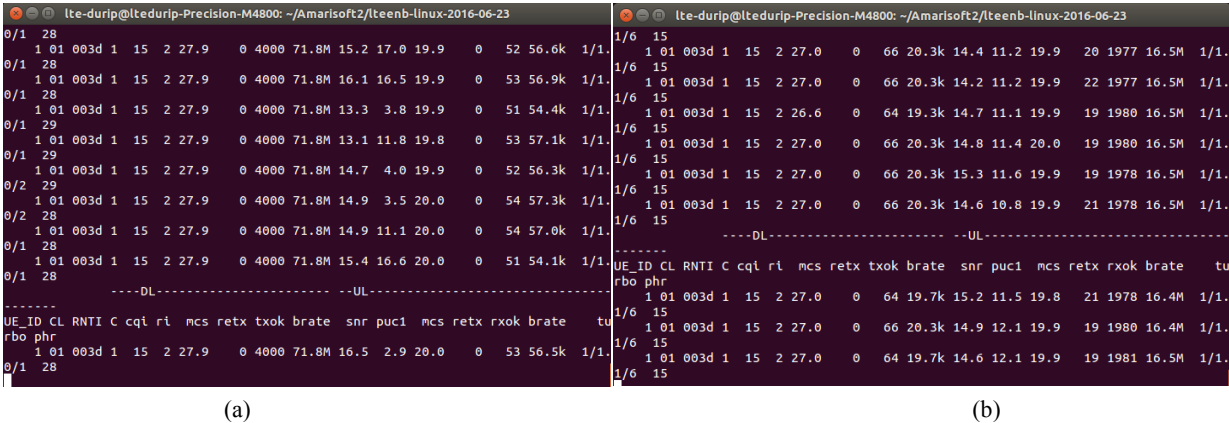


Figure E.4: Amarisoft eNodeB's MAC trace for (a) DL and (b) UL during measurement with 10 MHz BW and 2x2 MIMO.

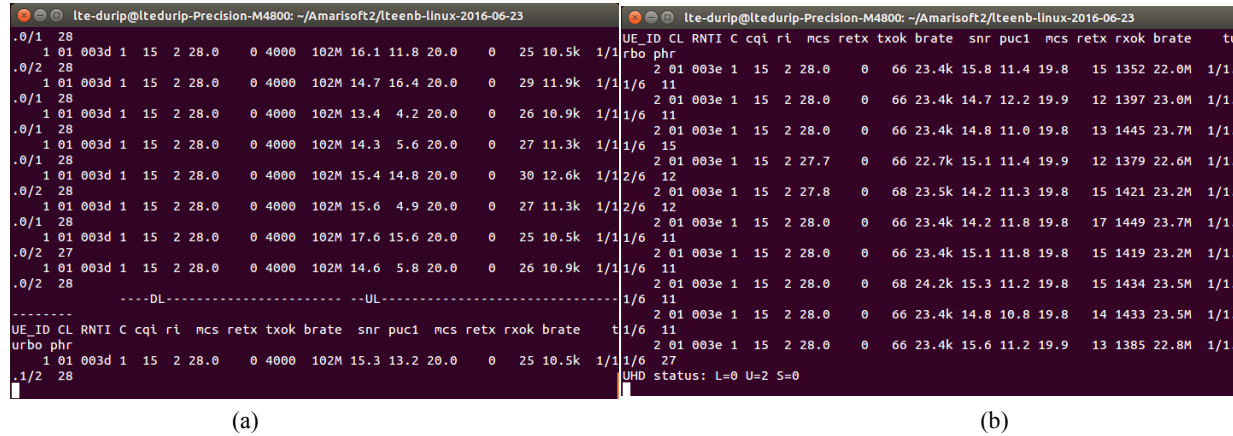


Figure E.5: Amarisoft eNodeB's MAC trace for (a) DL and (b) UL during measurement with 20 MHz BW and 2x2 MIMO.

Table E.2 presents a summary of the measurements carried out for the different LTE bandwidths and compares the average measured throughput against the expected theoretical peak throughput calculated using the 3GPP specifications (Appendix B). The process of calculating the average throughput on DL and UL can be understood by considering the example of 2x2 LTE MIMO with 5 MHz BW as follows:

- The total data transferred on the DL during 100 s is found to be 371 MB, 371.17 MB and 371.1 MB respectively for the three trials. Considering the average of the data transferred as 370.09 MB, the average measured throughput can be computed as $= (370.09 \text{ MB} * 8 \text{ bits}) / 100 \text{ s} = 29.61 \text{ Mb/s}$. This is in very close agreement to the expected theoretical throughput of 31.704 Mb/s for the same bandwidth and MCS values (cf. Table B.4).
- The total data transferred on the UL during 100 s is found to be 103.35 MB, 103.03 MB and 103.30 MB respectively for the three trials. Considering the average of the data transferred as 103.23 MB, the average measured throughput can be computed as $= (103.23 \text{ MB} * 8 \text{ bits}) / 100 \text{ s} = 8.26 \text{ Mb/s}$. This is in close to the expected theoretical throughput of 10.680 Mb/s according to 3GPP for Category 3 UE with the same bandwidth and MCS values (cf. Table B.5).

Table E.2. Summary of throughput measurements for direct cabled setup with 2x2 MIMO.

Parameter		LTE Bandwidth					
		5 MHz		10 MHz		20 MHz	
		DL	UL ¹	DL	UL ¹	DL	UL ¹
Total Data Transfer in 100 s	Iteration 1	371 MB	103.35 MB	851.72 MB	205.45 MB	1.19 GB	285.94 MB
	Iteration 2	371.17 MB	103.03 MB	854.35 MB	205.11 MB	1.18 GB	285.54 MB
	Iteration 3	371.1 MB	103.30 MB	855.99 MB	206 MB	1.19 GB	284.88 MB
Rank indicator		2	2	2	2	2	2
Maximum MCS from Amarisoft eNB		27	20	27.9	20	28	20
Average Data Transfer		370.09 MB	103.23 MB	854.02 MB	205.52 MB	1.1867 GB	285.45 MB
Average Measured Throughput		29.61 Mb/s	8.26 Mb/s	68.32 Mb/s	16.44 Mb/s	97.21 Mb/s	22.836 Mb/s
Maximum Instantaneous Throughput from Amarisoft eNB		31.1 Mb/s	8.28 Mb/s	71.8 Mb/s	16.5 Mb/s	102 Mb/s	22 Mb/s
Theoretical Throughput for this combination of MCS and BW calculated from 3GPP specs for Cat 3 UEs		31.704 Mb/s	10.680 Mb/s	75.376 Mb/s	21.384 Mb/s	102 Mb/s ²	43.816 Mb/s

¹ Category 3 UEs do not support two-layer spatial multiplexing on the uplink.

² Category 3 UEs are limited to a maximum DL data rate of ~100 Mbits/sec.

E.4 Conclusions

Analysis - Downlink Data

- In general, the rule of thumb throughput calculations, assuming no coding and a 25 % signaling overhead closely match the Transport block size-based calculations from 3GPP specs. Exceptions exists, such as for Cat. 3 UEs, which can achieve only ~100 Mbps on the 2x2 MIMO DL.
- Our measurements show a DL data rate of ~30 Mbps for 2x2 MIMO and 5 MHz LTE, which approximates the theoretical ~31.7 Mbps. For the SISO case, our measurements show a rate of ~15 Mbps which is half of the 2x2 MIMO throughput.
- For the 5 MHz measurements, the reported MCS was 27 as opposed to 28, which explains the lower than expected throughput.
- Our measurements show a DL data rate of ~70 Mbps for 2x2 MIMO and 10 MHz LTE, which approximates the theoretical ~75 Mbps. For the SISO case, our measurements show a rate of ~35 Mbps which is about half the 2x2 MIMO throughput.
- With 20 MHz LTE, our measurements show a DL data rate of 97.21 Mb/s, which closely approximates the theoretical peak data rate of 102 Mbits/sec for Cat. 3 UEs.
- The RSRP for the three cases of 5, 10 and 20 MHz is found to be -83 dBm, -86 dBm and -91 dBm respectively. Since the same total transmitted power is spread among twice as many resource elements for 2x bandwidth, we observe an average power drop of 3 dB. Note that the RSRP is measured on the reference signal, which is regularly spread across the LTE time-frequency resource grid.

Analysis - Uplink Data

- In general, the rule of thumb throughput calculations, assuming no coding and a 25% signaling overhead closely match the Transport block size-based calculations from 3GPP specs.
- Cat. 3 UEs do not use 64-QAM in the uplink and do not operate in MIMO mode [E.1].
- The theoretical maximum UL throughput for Cat 3. UEs is ~50 Mb/s.
- For 10 MHz bandwidth, our measured UL throughput rate is 16.44 Mb/s which is lower than the expected 21.384 Mb/s calculated using the specifications sheet.
- We observe that as the bandwidth increases, the mismatch between the expected and actual throughput becomes larger. For 20 MHz bandwidth, our measured UL throughput rate of 22.836 Mb/s is considerably lower than the expected theoretical rate of 43.816 Mb/s.

References

[E.1] Bing, Benny. *Broadband wireless multimedia networks*, Wiley, a John Wiley & Sons Inc., Publication, Hoboken, New Jersey, 2013;2012.

Appendix F

Initial Measurements for 2x2 LTE-MIMO: Over-the-Air Mode

This section describes the testing process and results from our LTE over-the-air (OTA) radiation trails when placing the eNodeB antennas and the UE in a shielded box. The use of a shielded box allows for these measurements to be carried out without creating interference or getting disturbed by other users operating on the same band.

F.1 Test setup

The setup used for carrying out the OTA measurements is as shown in Figure F.1. The USRP, which is part of the eNodeB, and the UE are both placed inside a shielded box. The USRP uses two short monopole antennas connected to its two Tx/Rx ports, whereas the Rogers AC330U UE uses its internal antennas. The shielded box has dimensions of approximately 60 cm x 50 cm x 30 cm and provides for small mechanical cutouts in one of its walls to allow cables to access the USRP and UE.

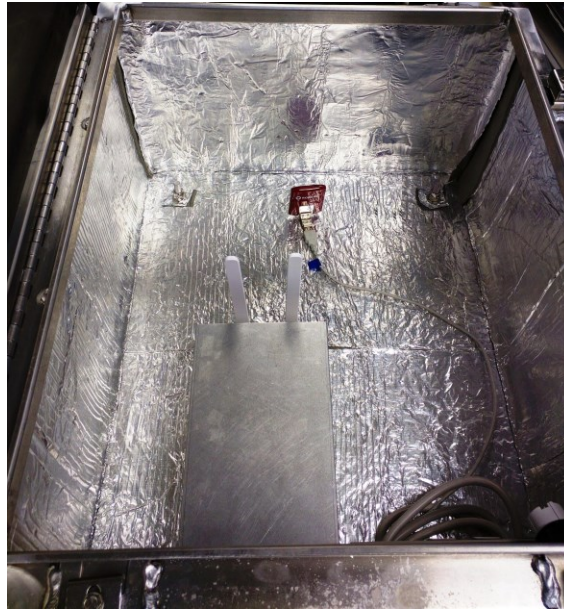


Figure F.1: Use of shielded enclosure for OTA MIMO measurements. UE uses its two internal antennas and is connected via USB cable to a mobile workstation for power and data logging.

F.2 Test methodology and procedure

The procedure followed to compute the average measured data rate on the DL and UL is same as that followed in case of the cabled setup and as described in Section E.2 of Appendix E. Given the uncertainty of the wireless channel, we consider doing more measurement iterations for averaging. It was observed that 10 iterations gave us stable values for the UL and 5 iterations for the DL.

In order to ensure a common scale with the earlier measurements, the analog gains of the USRP front end are adjusted by tweaking the parameters ‘*tx_gain*’ and ‘*rf_gain*’ on Amarisoft to achieve a RSRP of -83 dBm at the UE for the 5 MHz case. The values of the analog gains for this case are found to be higher than those for the cabled setup because of the higher path losses. Once the satisfactory values of RSRP are achieved, the gains are not modified when carrying out measurements for the 10 and 20 MHz bandwidth. For these cases, the RSRP is found to be -86 dBm and -89 dBm, which correspond to the earlier cases.

F.3 Results

As experienced earlier with the cabled setup, the throughput also ramps up and take a short, but non-negligible time to reach the maximum rate. After the initial ramp, the throughput remains fairly consistent until the end of the data transfer and then gradually drops to the minimum value.

Figures F.3 to F.5 show the Amarisoft eNodeB’s MAC traces during the measurements for 5, 10 and 20 MHz BW. The left half of the log indicates the parameter values for the DL and the right half corresponds to the UL. The throughput as indicated by the ‘*brate*’ column in the log shows a fairly consistent value during the measurement, after the initial ramp-up phase. Other parameters during the measurements such as the channel quality indicator (CQI), Rank Indicator (RI), and modulation and coding scheme (MCS) can also be observed.

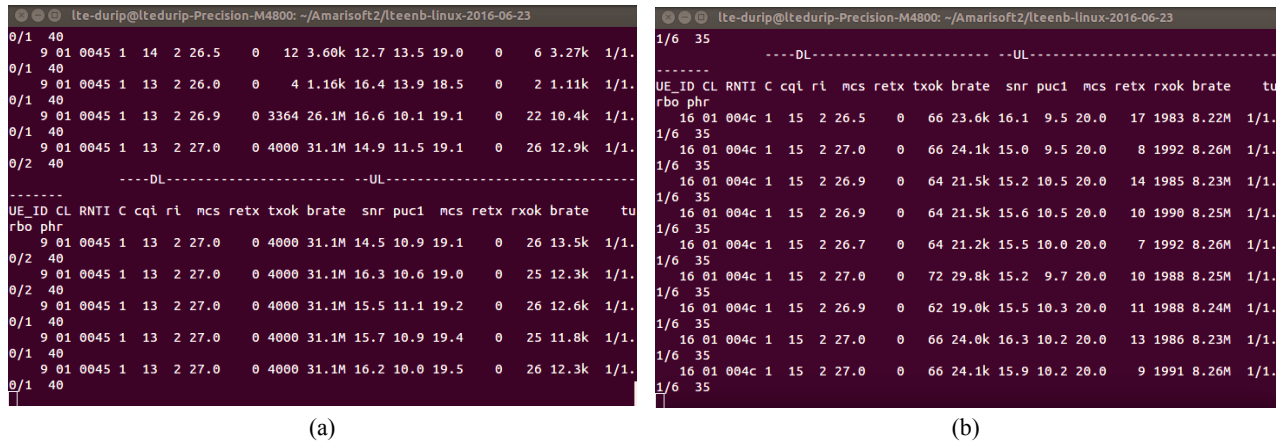


Figure F.3: Amarisoft eNodeB’s MAC trace for (a) DL and (b) UL for OTA DL measurement with 5 MHz BW and 2x2 MIMO.

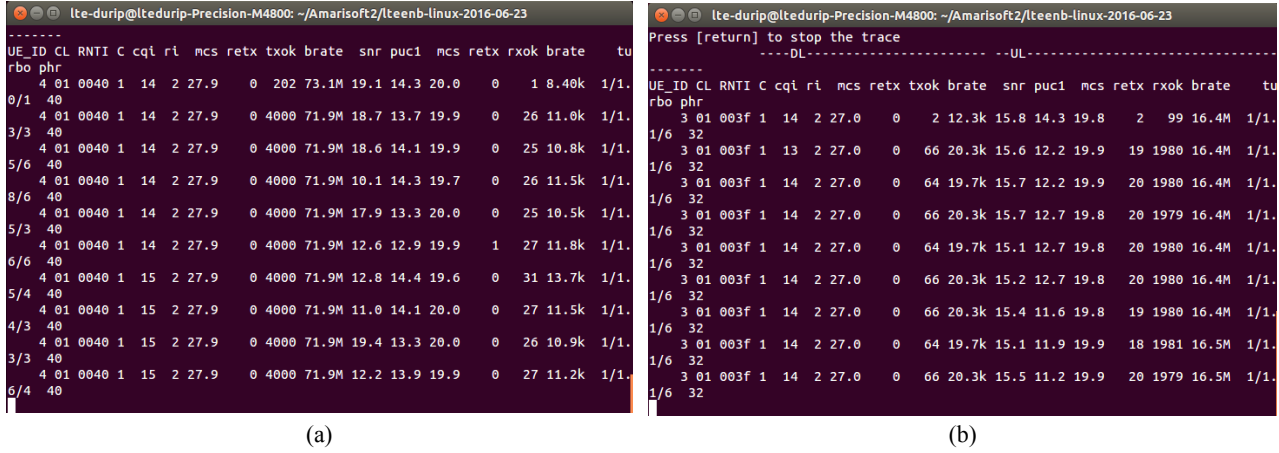


Figure F.4: Amarisoft eNodeB's MAC trace for (a) DL and (b) UL for OTA DL measurement with 10 MHz BW and 2x2 MIMO.

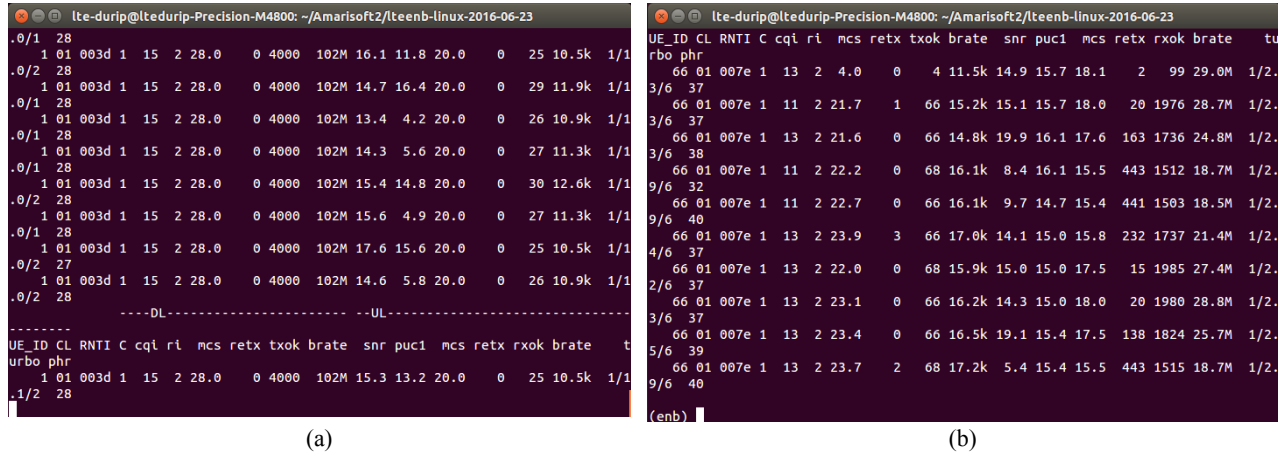


Figure F.5: Amarisoft eNodeB's MAC trace for (a) DL and (b) UL for OTA DL measurement with 20 MHz BW and 2x2 MIMO.

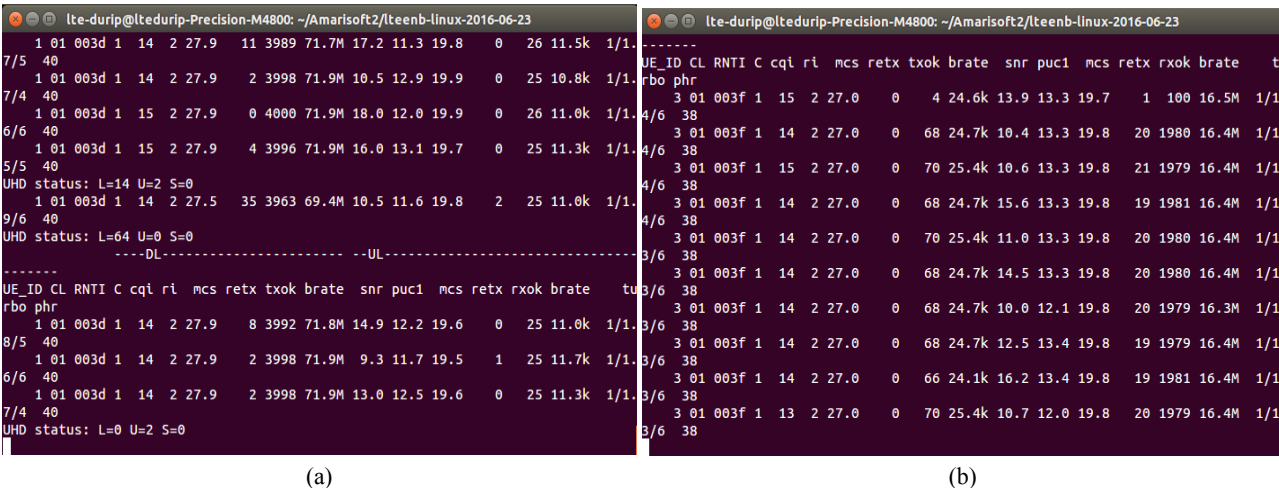


Figure F.6: Amarisoft eNodeB's MAC trace for (a) DL and (b) UL for OTA DL measurement with 10 MHz BW and 2x2 MIMO for Transmission Mode 4 operation.

Table F.1 summarizes the throughput measurements carried out for different LTE bandwidths for the OTA setup and LTE Transmission Mode 3. For 10 MHz bandwidth, we also measured the throughput for Transmission Mode 4.

Table F.1. Summary of throughput measurements for OTA 2x2 MIMO measurements.

Parameter		LTE Bandwidths							
		5 MHz (Transmission Mode 3)		10 MHz (Transmission Mode 3)		20 MHz (Transmission Mode 3)		10 MHz (Transmission Mode 4)	
		DL	UL ¹	DL	UL ¹	DL ²	UL ¹	DL	UL ¹
Total Data Transfer in 100 s	Iteration 1	368.94 MB	85.98 MB	842.14 MB	172.97 MB	1.18 GB	315.6 MB	851.71 MB	129.88 MB
	Iteration 2	369.23 MB	81.29 MB	848.10 MB	187.43 MB	1.19 GB	303.7 MB	846.29 MB	130.86 MB
	Iteration 3	370.52 MB	67.05 MB	839.27 MB	205.52 MB	1.19 GB	255.4 MB	851.28 MB	161.63 MB
	Iteration 4	370.39 MB	100.84 MB	847.74 MB	183.32 MB	1.19 GB	268.38 MB	848.76 MB	188.2 MB
	Iteration 5	370.35 MB	100.89 MB	850.86 MB	198.65 MB	1.19 GB	305.41 MB	789.56 MB	129.6 MB
	Iteration 6	---	101.82 MB	---	188.47 MB	---	296.75 MB	---	155 MB
	Iteration 7	---	102.80 MB	---	168.92 MB	---	287.21 MB	---	129.48 MB
	Iteration 8	---	67.9 MB	---	205.55 MB	---	278.66 MB	---	200.56 MB
	Iteration 9	---	68.38 MB	---	188.19 MB	---	281.1 MB	---	130.02 MB
	Iteration 10	---	66.7 MB	---	180.24 MB	---	293 MB	---	166.84 MB
Rank indicator		2	2	2	2	2	2	2	2
Maximum MCS from Amarisoft		27	20	27.9	20	28	18.1	27.9	15.9
Average Data Transfer		369.89 MB	84.37 MB	845.62 MB	187.93 MB	1.188 GB	288.52 MB	837.52 MB	152.21 MB
Average Measured Throughput		29.59 Mb/s	6.75 Mb/s	67.65 Mb/s	15.03 Mb/s	97.32 Mb/s	23.08 Mb/s	67 Mb/s	12.18 Mb/s
Maximum Instantaneous Throughput from Amarisoft eNB		31.1 Mb/s	8.25 Mb/s	71.9 Mb/s	16.5 Mb/s	103 Mb/s	29 Mb/s	71.9 Mb/s	16.4 Mb/s
Theoretical Throughput for combination of MCS & BW calculated from 3GPP specs for Cat 3 UE		31.704 Mb/s	10.680 Mb/s	75.6 Mb/s	21.384 Mb/s	102 Mb/s	43.816 Mb/s	---	---
Average Measured Throughput for the Cabled Mode (c.f. Table E.2)		29.61 Mb/s	8.26 Mb/s	68.32 Mb/s	16.44 Mb/s	97.21 Mb/s	22.836 Mb/s	---	---

¹ Cat. 3 UEs do not support two-layer spatial multiplexing in UL.

² Cat. 3 UEs are limited to a maximum DL data rate of ~100 Mb/s.

F.4 Observations and Conclusions

Analysis - Downlink Data

- Although this is an OTA setup and ideally isolated channels cannot be created, there are enough scatterers in the environment to get full performance of the 2x2 spatial multiplexing on the DL.
- Our measurements show a DL data rate of ~30 Mbps for 2x2 MIMO and 5 MHz LTE, which approximates the theoretical ~31.704 Mbps. For the SISO case, our measurements show a rate of ~15 Mbps which is half of the 2x2 MIMO throughput.
- Our measurements show a DL data rate of ~67.7 Mbps for 2x2 MIMO and 10 MHz LTE, which approximates the theoretical ~75 Mbps. For the SISO case, our measurements show a rate of ~35 Mbps which is about half the 2x2 MIMO throughput.
- With 20 MHz LTE, our measurements show a DL data rate of 97.32 Mb/s, which closely approximates the maximum data rate of 102 Mbits/sec that is achievable using a Cat. 3 UE.
- The DL throughput values obtained with the OTA setup are found to be equal to or slightly lower than the throughput values obtained with the cabled setup.
- For the DL, the throughput values obtained for both Transmission Mode 3 and 4 are nearly identical, and in close agreement with the expected rates.
- During the course of the measurement the RSRP values reported by the UE are found to lie within +/- 1 dBm of these values, but consistently scale with bandwidth.

Analysis - Uplink Data

- A greater variation in the measured throughput is observed for the UL than for the DL.
- Cat. 3 UEs do not use 64-QAM in the uplink and do not operate in MIMO mode [F.1] and, hence, the theoretical maximum UL throughput is ~50 Mbps.
- For 5 MHz bandwidth, our measured UL throughput rate is 6.75 Mb/s which is lower than the expected value of 10.680 Mb/s.
- For 10 MHz bandwidth, our measured UL throughput rate of 15.03 Mbits/s is lower than the expected theoretical rate of 21.384 Mbits/s.
- For 20 MHz bandwidth, our measured UL throughput rate of 23.08 Mb/s is considerably lower than the expected theoretical rate of 43.816 Mb/s.
- For the UL, the throughput values obtained for both Transmission Mode 3 and 4 are nearly identical, and lower than the expected rates.

References

[F.1] UE Categories, <https://en.wikipedia.org/wiki/E-UTRA>

Appendix G

Initial Measurements for 2x2 LTE-MIMO: Channel Emulation Mode

This section describes the testing process and results from the trials carried out using the channel emulator RFnest. The use of a channel emulator allows for the creation of a controlled RF environment, approximating ideal as well as non-ideal conditions between the transmit and receive antennas by controlling the attenuation on each link independently.

G.1 Test setup

The setup used for carrying out measurements with RFnest is as follows: The two TX/RX ports of the USRP that are part of the eNodeB are connected to RFnest ports 1 and 2 and the two antenna terminals of the UE are connected to RFnest ports 3 and 4.

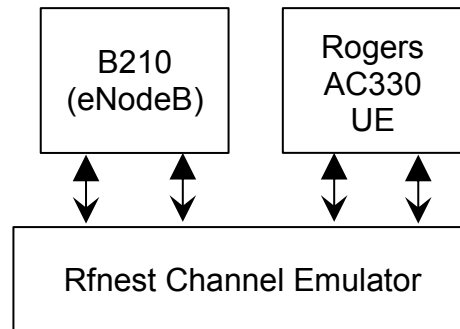


Figure G.1: Setup used for emulating non-ideal channels using Rfnest hardware for 2x2 MIMO measurements.

It is a good practice to have additional attenuation of around 20 dB in each of the paths to prevent the RFnest ports from possible damage due to high power UL.

Table G.2. Summary of RFnest port connections.

	RFnest Ports			
In hardware	1	2	3	4
In software	0	1	2	3
Connections	TX/RX Port A of B210 (eNodeB Antenna 1)	TX/RX Port B of B210 (eNodeB Antenna 1)	Antenna Terminals of Rogers AC330 UE (UE Antenna 1)	Antenna Terminal 2 of Rogers AC330 UE (UE Antenna 2)

G.2 Test methodology

The procedure followed to compute the average measured data rate on the DL and UL is same as that followed in case of the cabled setup and as described in Section E.2 of Appendix E. In order to ensure a common scale with the earlier measurements, the analog gains of the USRP front end are adjusted by tweaking the parameters '*tx_gain*' and '*rx_gain*' on Amarisoft to achieve a RSRP of -83 dBm at the UE for the 5 MHz case. The values of the analog gains for this case are found to be higher than those for the cabled setup because of the additional base attenuation of the RFnest and the fixed discrete attenuators that we put on its ports for protecting the equipment. Once the satisfactory values of RSRP were achieved, the gains were not modified for carrying out measurements for the 10 and 20 MHz bandwidth.

In the RFview GUI, for the first trial we set the gain between any pair of ports, i.e. (eNB1,UE1), (eNB1,UE2), (eNB2,UE1), (eNB2,UE2), (eNB1,eNB2) and (UE1,UE2) to 0 dB. This is to emulate that any path between the two transmit antennas and the two receive antennas experiences the same attenuation and the same channel. The measured data for the attenuation introduced by the setup can be found in Appendix H.

G.3 Results

As observed in all throughput measurements, the data rate on both DL and UL is found to initially ramp-up as the UE has to buffer data and request resources from the eNodeB. Similarly, a ramp-down phase is also observed towards the end of the data transfer.

Figures G.2 shows the Amarisoft eNodeB's MAC trace during the DL measurements for 5 MHz bandwidth.

```

ltdurip@ltdurip-Precision-M4800: ~/Amarisoft2/teenb-linux-2016-06-23
UE_ID CL RNTI C cqi ri mcs retx txok brate snr puc1 mcs retx rxok brate tu
rbo phr
17 01 004d 1 15 2 27.0 0 144 21.7M 12.3 11.6 15.0 0 1 2.80k 1/1.
0/1 1
17 01 004d 1 15 2 27.0 2 2898 21.6M 13.8 11.5 15.1 0 29 3.77k 1/1.
0/1 0
17 01 004d 1 15 2 27.0 1 2881 21.5M 12.4 11.0 14.9 0 28 3.56k 1/1.
0/1 1
17 01 004d 1 15 2 27.0 0 2888 21.5M 13.4 10.7 14.9 0 25 3.16k 1/1.
0/1 1
17 01 004d 1 15 2 27.0 1 2887 21.6M 13.9 11.2 14.7 0 29 3.57k 1/1.
0/1 0
17 01 004d 1 15 2 27.0 0 2880 21.5M 13.5 11.3 14.6 0 25 3.06k 1/1.
0/1 0
17 01 004d 1 15 2 27.0 0 2888 21.5M 11.0 10.9 15.2 0 28 3.69k 1/1.
0/2 1
17 01 004d 1 15 2 27.0 2 2884 21.6M 12.7 11.8 15.0 0 29 3.68k 1/1.
0/1 1
17 01 004d 1 15 2 27.0 2 2884 21.5M 12.3 10.1 14.8 0 27 3.38k 1/1.
0/1 1
17 01 004d 1 15 2 27.0 2 2890 21.6M 11.0 11.0 14.9 0 25 3.18k 1/1.
0/1 0
UHD status: L=0 U=1 S=0

```

Figure G.2: Amarisoft eNodeB's MAC trace for DL during measurement with RFnest for 10 MHz BW and 2x2 MIMO.

Table G.2 presents a summary of the throughput measured on DL for 2x2 MIMO for the RFnest channel. We observe lower values than expected for perfect conditions but still some MIMO gain.

Table G.2. Summary of throughput measurements on DL for 5 MHz bandwidth and 2x2 MIMO with RFnest.

Parameter		DL
Total Data Transfer in 100s	Iteration 1	255.09 MB
	Iteration 2	255.09 MB
	Iteration 3	267.40 MB
Rank indicator		2
Maximum MCS from Amarisoft eNB		27
Average Data Transfer		259.19 MB
Average Measured Throughput		20.74 Mb/s
Maximum Instantaneous Throughput from Amarisoft eNB		21.6 Mb/s
Theoretical Throughput for this combination of MCS and BW calculated from 3GPP specs		31.704 Mb/s

G.4 Conclusions

Analysis - Downlink Data

- Our measurements show a DL data rate of ~21 Mbps for 2x2 MIMO and 5 MHz LTE, which is lower than the theoretical ~31.7 Mbps.
- Increasing the gain on the analog front ends leads to increased UE disconnection during the measurements.

Appendix H

RFnest Attenuation Data

This section presents measured attenuation data between two ports for the RFnest channel emulator.

H.1 Measurement Setup & Methodology

Figure H.1 shows a block diagram of the setup used to characterize the attenuation between the two ports of the RFnest hardware for different values of attenuation on the GUI. The CMW500 is used as a signal generator to get a 0 dBm signal at 2600 MHz centre frequency that is fed to Port 4 of the RFnest, and a spectrum analyzer is used to measure the received signal amplitude at Port 8. Any two ports can be chosen for the measurements, as long as they are correspondingly selected in the scenario.

In the RFview scenario, a path is created between the two selected ports and the channel attenuation is adjusted manually. The observed value of the signal amplitude after compensating for the loss introduced by the cables and adapters is the attenuation introduced by the RFnest hardware.

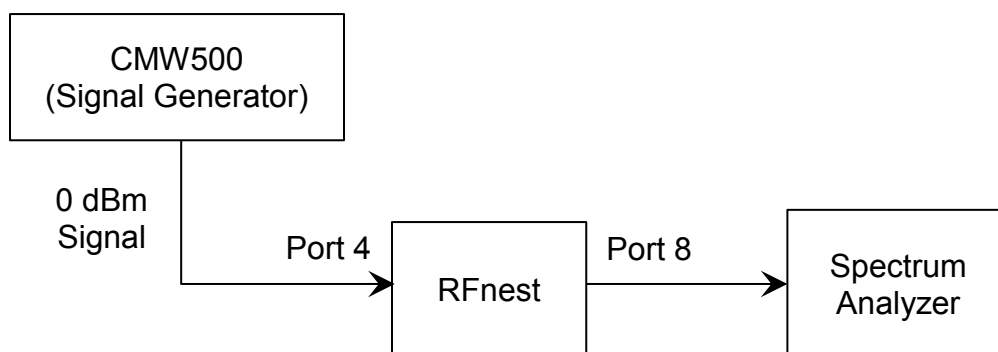


Figure H.1: Measurement setup used for characterizing the attenuation introduced by RFnest.

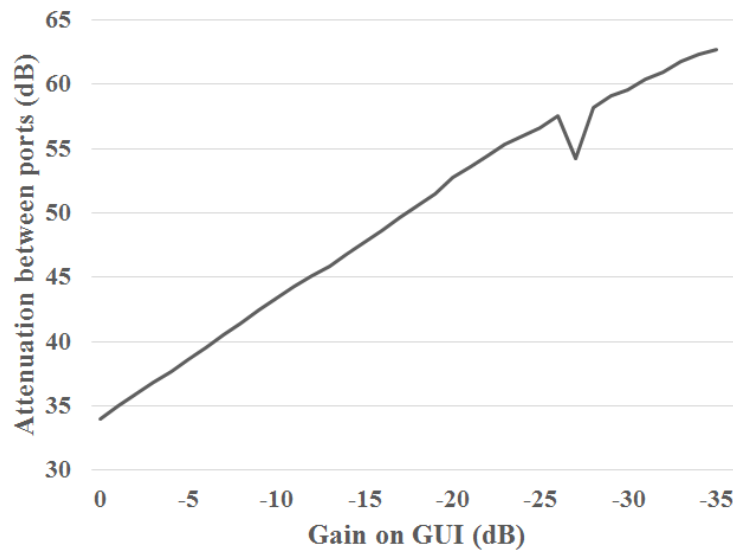
H.2 Results

The attenuation introduced by the hardware can be increased by reducing the ‘Gain’ parameter on the RFview GUI. Table H.1 summarizes the attenuation values measured for different values of gain on the GUI. Figure H.1 highlights the linear behavior of the hardware.

With a Gain of 0 dB on the GUI, the hardware introduces an attenuation of at least 34 dB in the path.

Table H.1. Summary of attenuation measurements with RFnest.

Gain on GUI (dB)	Attenuation (dB)	Gain on GUI (dB)	Attenuation (dB)	Gain on GUI (dB)	Attenuation (dB)	Gain on GUI (dB)	Attenuation (dB)	Gain on GUI (dB)	Attenuation (dB)	Gain on GUI (dB)	Attenuation (dB)
0	34	-6	39.48	-12	45.07	-18	50.5	-24	55.95	-30	59.6
-1	34.95	-7	40.48	-13	45.81	-19	51.43	-25	56.63	-31	60.38
-2	35.88	-8	41.43	-14	46.74	-20	52.79	-26	57.52	-32	60.92
-3	36.87	-9	42.4	-15	47.66	-21	53.62	-27	54.19	-33	61.76
-4	37.67	-10	43.35	-16	48.62	-22	54.43	-28	58.2	-34	62.35
-5	38.54	-11	44.24	-17	49.59	-23	55.3	-29	59.13	-35	62.73

**Figure H.1:** Measured attenuation between two ports on RFnest for different values of gain.

H.3 Conclusion

The RFnest hardware has a fairly linear attenuation performance with respect to the values set on the GUI. The minimum attenuation introduced between the two ports is ~34 dB.

Appendix I

Software Development for the Testbed

This section describes the features to be included in the software developed for the testbed. Broadly, the goals of the software development are:

1. Improve testbed user's experience
2. Easier maintenance and supervision by administrators
3. Scheduling, sharing and management of resources
4. Safety, Security, Control of user privileges

Suggested features and functionalities:

1. **Intuitive:** The software should be intuitive and easy-to-navigate for a new user. We should start from the basics to ensure smooth, easy and safe operation and then offer more sophisticated software services. This could be supported with help files, tutorials and simple guidelines in the form of tooltips.
2. **Platform:** A user might prefer to check his smartphone or tablet for quick updates on his experiments. It would be highly advantageous if the GUI could work equally well across multiple devices.
3. **Control:** The testbed should allow access to registered and authenticated users. Additionally, testbed administrators should have complete control over the testbed (on-site or remotely) at all times.

What is needed first is providing easy and safe user access, where the user cannot break anything and where we can flush if he does.

4. **Reset and Self Test :** A script that checks the testbed components and brings them in a known initial state (essentially flashing the testbed when a user finishes his slot). A script might then be created and loaded to configure the testbed at the beginning of the reservation --> future proposal that can manage all our testbeds.

Additionally, even during the measurement slot, there should be provision for the user to 'Reset' and bring the system to its initial stage.

5. **Monitoring:** The software should include tools for monitoring experiments and critical LTE signaling parameters (e.g. is the LTE system actually up--we had some issues with stability of Amarisoft/USRPs) --> either real-time (ideally visual) or log-files.

The software could also monitor and log the user's data usage, and any attempts to accessing and modifying the file system, and source installations.

6. **Automated alerts:** The software could monitor a set of parameters obtained from the hardware, and in case of any unexpected values that could interfere or damage any component, alert the user and administrators. The alerts could be in the form of a prompt, pop-up or an email. Testing could be suspended until the anomaly is resolved.
7. **Requests from users:** The software should have a feature where users could plan their experiments and request resources from the administrators. Typically, these would be:
 - a. Time slots for experiments
 - b. Hardware devices to be used
 - c. Software packages to be used
 - d. Any additional software that the user would want installed on the PC (maybe temporarily).

A GUI for customizing the components that a user wants to involve in the experiment. From this system-level GUI, a user might need to do some command line configurations (Amarisoft) or use GUIs provided by the vendors (RFnest, CMW500, UE, filters, switches, etc.), but it would be nice if the user would be brought there from a visually well organized system-level portal.

Next step would be to export this portal to the Web so that future users could see and plan experiments in advance.

8. **Results:** A user would be interested in a number of parameters and they would be spread across the output of many different GUIs. The software should have a feature where the results could be integrated, compared, saved and exported in different formats.
9. **Programming Capabilities:** The software could allow the user to carry out basic programming to process the data - for example to average across values, find maximum/minimum values, make plots etc. This could be achieved by allowing the user access to command line tools in C++/Python in a controlled manner.
10. **Software standards:** The software development should adhere to standard software development guidelines. Additionally, test cases and beta testing of the software should be carried out with a listing of identified bugs.

There should be a provision for support and maintenance of the software system.

Appendix J

CMW500 License Keys

Figure J.1 shows the active license keys on the CMW500.

Active License Keys		
Show Category View	<input checked="" type="checkbox"/>	
[-] Device Identification	1201.0002K50-152659-wm	
Part No.:	1201.0002K50	
Serial Number:	152659	
[-] Active License Keys		
[-] Universal		
KB036	Name	Lic.
Bundles	6 GHZ ENABLING	1
Protocol Test		
Tools		
[-] RF Test Signaling	Name	Lic.
KS500	LTE FDD R8 SIG BASIC	1
KS550	LTE TDD R8 SIG BASIC	1
KS650	WLAN A/B/G SIG BASIC	1
KS651	WLAN N SIG BASIC	1
[-] RF Test Measurements	Name	Lic.
KM010	SPECTRUM ANALYZER	1
KM500	LTE FDD R8 TX MEAS	1
KM550	LTE TDD R8 TX MEAS	1
KM650	WLAN ABG TX MEAS	1
KM651	WLAN N SISO TX MEAS	1
KN550	LTE TDD R9 ENODEB TX MEAS	1
RF Test Generator		
RF Test Fading		
Application Test		

Figure J.1: Active License Keys on CMW500 (as verified on 5th April, 2016).

Appendix K

FCC Experimental License Application Process

Introduction and Background

In order to ensure that the radio frequency spectrum may be shared efficiently by a large number of users the Federal Communications Commission (FCC) was established by Congress. The FCC established regulations that provided for segregated frequency bands which divide the spectrum according to usage. For example, audio broadcasting is allocated frequency bands around 1 MHz (AM) and 100 MHz (FM) while television broadcasting is allocated several frequency bands above 54 MHz but not including the 100 MHz audio broadcast band. Numerous other services compete for the spectrum including Public Safety, land mobile and common carriers (e.g. Cellular telephone)². Certain frequency bands are also reserved for Federal Government and Military use. Those frequencies are coordinated by other agencies such as the NTIA. Within the various frequency bands most services are allocated particular frequencies which are coordinated on a geographic basis to prevent interference within a local area. The ideas of frequency and geographic separation of users is the basis for almost all of our radio regulations. In order to regulate radio frequency usage the FCC provides a licensing system where applications are reviewed for compliance with the regulations. If approved, a license is issued for a specific time period. Particular frequencies, locations and modes of operations are specified in the license.

In addition to the usual radio services, the FCC provides for an experimental radio service. An experimental radio license is issued to those who have a specific need to use a portion of the radio spectrum either to conduct radio experiments or where radio is required as a part of an experimental system³. Experimental radio is administered through the FCC Office of Engineering Technology (OET). The CAER Cognitive Radio Testbed and CORNET are examples of systems requiring an experimental license.

Obtaining an Experimental License

Experimental radio is administered through the FCC Office of Engineering Technology (OET). Applicants for experimental licenses use an online Experimental Licensing System (ELS)⁴. (Other online systems are used for Commercial and Amateur radio services.) For experiments lasting 6 months or less an application for a Special Temporary Authorization (STA) should be made. For longer term experiments an Experimental License should be requested. The Experimental license procedure is described below.

Obtain a FRN

Before applying it is necessary to get a FCC Registration Number (FRN) which identifies the applicant. The FRN may be obtained by registering online using the FCC CORES system⁵. The FRN should be recorded as it is used for all future FCC applications Business information, tax ID number and applicant

² Title 47 Code of Federal Regulations (CFR), http://www.ecfr.gov/cgi-bin/text-idx?SID=a3ca4e7e75b40503be19b91c4a188323&tpl=/ecfrbrowse/Title47/47tab_02.tpl

³ Title 47 CFR Chapter 1A subpart 5, http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=a3ca4e7e75b40503be19b91c4a188323&tpl=/ecfrbrowse/Title47/47cfr5_main_02.tpl

⁴ <https://apps.fcc.gov/oetcf/els/index.cfm>

⁵ <https://apps.fcc.gov/coreWeb/publicHome.do>

information are required for the FRN application. The FRN is public information. . There is a search engine that allows the FRN to be found if it is lost. A required password should also be recorded as it is required to edit the FRN information.

Application Process

Start at the index page: <https://apps.fcc.gov/oetcf/els/index.cfm>

Under the “Miscellaneous” menu heading select “User Guide” to view a comprehensive manual for the licensing process.

A practice application site is provided to help users to learn the process. Data entered at the practice site will not be processed by the FCC. The practice site can be accessed through the hyperlink on the index page labeled “the Experimental Licensing System test site”.

Select: “Form 442 - New License/Modification of License”. On the new page select new application and enter your FRN then “proceed”.

Administrative Section Entry

On the new page you enter your contact information and answer a few questions on the nature of the experimental program. Additional descriptive information will be required depending on your answers to questions 4 through 7. That information should be placed in a PDF file and inserted at the end of the application process. For a “radio test-bed” the answers to questions 5, 6 and 9 are probably “no”. The FCC may not issue the license for the full term of planned operation. If not you will be able to renew the license. “Proceed” to the next application page.

The following page “question 10” requests information on the transmitting equipment used in the experiment. Enter the Manufacturer, model and number of units. If the equipment is experimental indicate so as “yes”. For example: Manufacturer: Ettus Engineering, Model: E110, Number of units: 10, Experimental: Yes. Select either “enter more equipment” or “proceed”.

The next page contains questions 11 through 18. The answers to questions 11, 13 and 14 will probably be “no”. The answers to questions 15 and 17 will probably be “yes”.

The application is “signed” by typing your name in the appropriate box. The application is far from complete at this point though! “Proceed” to the next section.

File and Confirmation Numbers

At this point you will receive a “File Number” and a “confirmation number” it is very important to record those values as you won’t be able to restart the application process without them. If you close the web browser at this point you will need the numbers to log back into the application. They are also required to check the application status.

An outline of the technical data entry procedure is also given on this page. The technical data entry can be confusing and redundant. It may require several attempts before getting everything in order. “Proceed” to the next application page.

Antenna Registration Entry

The “Antenna Registration” page specifies the location of the antenna/radio used. There may be other antennas which are added on other application pages. For an indoor SDR test bed (depending on the configuration) it may be possible to treat all units as “mobile”. In that case enter the coordinates of the

building and a radius of operation that includes the entire building. “Directional Antenna” and “Antenna Height” questions are probably “no”. “Proceed” to the Antenna Frequency Registration.

Frequency Registration Entry

At this page it will be necessary to enter frequency bands and power levels that will be used by the transmitters. Frequency tolerance may be left blank if a wide band of frequencies is specified. A typical frequency range would be 3550-3650 MHz. Where possible it is good to use existing frequency band limits and emission types for a particular service as this avoids some coordination questions. If a restricted frequency band (such as an emergency frequency) is included in the frequency range it will probably be rejected. It probably isn't a good idea to include the whole spectrum in one line! Specify reasonable power levels. The antenna gain will probably be zero dBi or less so the ERP can be identical to the transmitter power 1W peak is probably a good value to choose for the test bed. You may use less than the specified amount of power. Continue to add frequencies as necessary by selecting the appropriate button. After all frequencies have been added you can continue by adding emissions to each frequency.

Emissions Entry

The emissions portion of the application requires the applicant to specify the type of modulation and bandwidth that will be used. Multiple emissions may be specified for each frequency band. Each frequency band must have at least one emission specified. This tends to make the application very complex in cases such as a SDR test-bed where many different emissions are to be tested. Fortunately, it is possible to request a modification to the license to add emissions at a later date. Once the emission is determined an emissions designator and bandwidth must be formulated. For example: F3E is a frequency modulated analog sound transmission. A copy of the emissions designator table is included as an Appendix to this report. Some emissions are more difficult to define, however. An accepted designator for a LTE signal is W7W which falls into the “cases not covered above” category. In cases where the emissions designator is not sufficient to describe the signal it may be necessary to attach an explanation to the application. The process is repeated until all frequencies and emissions are complete.

Attachments

Near the end of the application process is the attachment section. Attach any additional information here as appropriate. A PDF document is usually the best format. Some common attachments are listed here.

Experiment description or Government project information (as determined by application questions 4-7).

Stop buzzer page: gives the contact information in case the experiment must be terminated immediately.

Request for fee waiver: Educational and certain other agencies may request a fee waiver. Attach a text document (PDF) that explains the situation.

Fee Payment

Fee payment is required for most applicants. If a fee waiver has been requested the payment may be skipped. Otherwise the details are shown on the Fee Payment page of the application.

Processing the Application

Once the application has been completed the FCC will usually either grant it within a few weeks or ask for additional information. In cases where there are Government users of the frequencies requested the license application will be forwarded to the appropriate government agency for review. This review process takes additional time.

Example Application

The VT O-CORNET license, introduced below, is an example of what can be obtained through this process. Note that the license is very specific as to location, frequencies and emissions. There are also limitations or “Special Conditions” appended to the license. Typically the Special Conditions contain a statement that the experimental station must cease operation if it causes interference. Another typical statement omits the frequency tolerance requirement. Another typical condition statement is that the experimental user must coordinate with other users before operating on the frequency. These conditions effectively make the experimental license secondary to all other licenses and subject to termination if any interference occurs.

FCC Experimental License

Our experimental FCC license for the campus-wide O-CORNET testbed covers several bands as indicated in the table below.

Table K.1: Frequency bands and transmission parameters for FCC experimental license for fixed, mobile and portable O-CORNET SDR nodes (see also <https://apps.fcc.gov/els/GetAtt.html?id=154653&x=>).

Frequency [MHz]	Data Type	Modulation	Max. channel bandwidth [MHz]
450 - 512	Digital, Analog	BPSK, QPSK, QAM, A0, F2, F3, 1M40W7W (OFDM, LTE)	1.4 (LTE)
764 – 862 (98 MHz)	Digital, Analog	BPSK, QPSK, QAM, A0, F2, F3, 1M40W7W (OFDM, LTE)	1.4 (LTE)
869 - 894	Digital, Analog	BPSK, QPSK, QAM, A0, F2, 1M40W7W (OFDM, LTE)	1.4 (LTE)
902 - 928 (ISM 1)	Digital, Analog	BPSK, QPSK, QAM, A0, A3, F2, F3, 1M40W7W (OFDM, LTE)	1.4 (LTE)
2000 - 2100	Digital, Analog	BPSK, QPSK, QAM, A0, F2, F3, 10M0W7W (OFDM, LTE)	10 (LTE)
3400 - 3550	Digital, Analog	QPSK, 16QAM, 64QAM, A0, F2, F3, 3M00P0N, 40M0W7W (OFDM, LTE)	40 (LTE) 3 (pulse)
3550 - 3650	Digital, Analog	QPSK, 16QAM, 64QAM, 256QAM, A0, F2, F3, 3M00P0N, 40M0W7W (OFDM, LTE)	40 (LTE) 3 (pulse)

F2: FSK

F3: FM

A0: unmodulated (single tone)

A3: AM, including single-sideband voice

3M00P0N: Unmodulated pulse, 3 MHz bandwidth

5M00W7W, 10M0W7W: OFDMA 5 MHz and 10 MHz

Emission types: http://wireless.fcc.gov/services/index.htm?job=licensing_2&id=industrial_business
http://www.comreg.ie/_fileupload/publications/ComReg0834.pdf

Appendix L

FCC Emissions Table

§ 2.201 Emission, modulation, and transmission characteristics.

The following system of designating emission, modulation, and transmission characteristics shall be employed.

- (a) Emissions are designated according to their classification and their necessary bandwidth.
- (b) Three symbols are used to describe the basic characteristics of emissions. Emissions are classified and symbolized according to the following characteristics:
 - (1) First symbol—type of modulation of the main carrier;
 - (2) Second symbol—nature of signal(s) modulating the main carrier;
 - (3) Third symbol—type of information to be transmitted.

Note to paragraph (b): Two additional symbols for the classification of emissions may be added for a more complete description of an emission. *See* Appendix 1, Sub-Section IIB of the ITU *Radio Regulations* for the specifications of these fourth and fifth symbols. Use of these symbols is not required by the Commission.

(c) First Symbol—types of modulation of the main carrier:

(1) Emission of an unmodulated carrier	N
(2) Emission in which the main carrier is amplitude-modulated (including cases where sub-carriers are angle-modulated):	
—Double-sideband	A
—Single-sideband, full carrier	H
—Single-sideband, reduced or variable level carrier	R
—Single-sideband, suppressed carrier	J
—Independent sidebands	B
—Vestigial sideband	C
(3) Emission in which the main carrier is angle-modulated:	
—Frequency modulation	F
—Phase modulation	G
(4) Emission in which the main carrier is amplitude and angle-modulated either simult. or in a pre-established sequence	D
(5) Emission of pulses: ¹	
—Sequence of unmodulated pulses	P
—A sequence of pulses:	
—Modulated in amplitude	K
—Modulated in width/duration	L
—Modulated in position/phase	M

—In which the carrier is angle-modulated during the period of the pulse	Q
—Which is a combination of the foregoing or is produced by other means	V
(6) Cases not covered above, in which an emission consists of the main carrier modulated, either simultaneously or in a pre-established sequence, in a combination of two or more of the following modes: amplitude, angle, pulse	W
(7) Cases not otherwise covered	X

¹ Emissions where the main carrier is directly modulated by a signal which has been coded into quantized form (e.g. pulse code modulation) should be designated under (2) or (3).

Note: Whenever frequency modulation “F” is indicated, Phase modulation “G” is also acceptable.

(d) Second Symbol—nature of signal(s) modulating the main carrier:

(1) No modulating signal	0
(2) A single channel containing quantized or digital information without the use of a modulating sub-carrier, excluding time-division multiplex	1
(3) A single channel containing quantized or digital information with the use of a modulating sub-carrier, excluding time-division multiplex	2
(4) A single channel containing analogue information	3
(5) Two or more channels containing quantized or digital information	7
(6) Two or more channels containing analogue information	8
(7) Composite system with one or more channels containing quantized or digital information, together with one or more channels containing analogue information	9
(8) Cases not otherwise covered	X

(e) Third Symbol—type of information² to be transmitted:

(1) No information transmitted	N
(2) Telegraphy—for aural reception	A
(3) Telegraphy—for automatic reception	B
(4) Facsimile	C
(5) Data transmission, telemetry, telecommand	D
(6) Telephony (including sound broadcasting)	E
(7) Television (video)	F
(8) Combination of the above	W
(9) Cases not otherwise covered	X

² In this context the word “information” does not include information of a constant, unvarying nature such as is provided by standard frequency emissions, continuous wave and pulse radars, etc.

(f) Type *B* emission: As an exception to the above principles, damped waves are symbolized in the Commission's rules and regulations as type *B* emission. The use of type *B* emissions is forbidden.

(g) Whenever the full designation of an emission is necessary, the symbol for that emission, as given above, shall be preceded by the necessary bandwidth of the emission as indicated in § 2.202(b)(1).

[49 FR 48697, Dec. 14, 1984, as amended at 75 FR 63030, Oct. 13, 2010]

Appendix M

Equipment List

Table P.1 provides the main equipment list and includes the components that have been assembled for the LTE-CORNET testbed and reassembled for the LTE-CORNET/COMWITS testbed presented in this report. Table P.2 lists the auxiliary equipment.

Table M.1. Main Equipment. The shaded rows indicate products that were obtained under ARO/DURIP grant # W911NF-14-1-0553.

Product	Source	#	Unit Price ⁶	Total Price
RFnest A208 (1.8-2.8 GHz)	Intelligent Automation Inc.	1	\$22,000	\$22,000
RFnest A208 (0-1.0 GHz)	Intelligent Automation Inc.	1	\$22,000	\$22,000
6.2 GHz Spectrum Analyzer	Tektronix SA2500, refurbished	2	\$6,273	\$12,546
1201.0002K50: CMW500 (Serial # 152659)	Rohde & Schwarz	1		
• CMW-PS503: CMW500 Basic Assembly (mainframe), 70MHz to 3.3GHz		1	\$10,024	\$10,024
• CMW-S100A (includes H100A): Baseband Measurement Unit, with 1GByte digitizer memory		1	\$2,511	\$2,511
• CMW-S550B (includes H550B): Baseband Interconnection, flexible link, for non-signaling, signaling and IQ access		1	\$1,383	\$1,383
• CMW-S570B (includes H570B): RF Converter (TRX)		1	\$7,004	\$7,004
• CMW-S590A (includes H590A): RF Frontend, basic functionality		1	\$1,463	\$1,463
• CMW-S600B (includes H600B): CMW500 frontpanel with display/keypad		1	\$1,422	\$1,422
• CMW-B300B (includes H300B): Signaling Unit Wideband, for WCDMA / LTE		1	\$10,684	\$10,684
• CMW-B620A (includes H620A): Digital Video Interface (DVI)		1	\$253	\$253
• CMW-KB036: Extended frequency range, 3.3 GHz to 6 GHz, per RF converter		1	\$6,496	\$6,496
• CMW-KM010: Spectrum analyzer, resolution bandwidth 100 Hz to 10 MHz		1	\$2,030	\$2,030
• CMW-KM550: LTE TDD (TD-LTE) Release 8, TX measurement, uplink		1	\$5,277	\$5,277
• CMW-KN550: LTE TDD Release 8/9, eNode B TX measurement, Downlink		1	\$4,062	\$4,062
• CMW-KS550: LTE TDD Rel. 8, signaling/network emulation, basic functionality		1	\$9,020	\$9,020
• CMW-KS525: LTE, user defined bands, signaling/network emulation, generic feature		2	\$5,316	\$10,632

⁶ Including discounts, where available

Product	Source	#	Unit Price ⁷	Total Price
• CMW-B200A: Signaling Unit Universal (SUU)		1	\$4,839	\$4,839
• CMW-B270A: Wimax/WLAN signaling module for SUU		1	\$2,661	\$2,661
• CMW-PK65: WLAN call box bundle (includes KM650/651, KS650/651)		1	\$13,113	\$13,113
• CMW-KM500: LTE FDD rel. 8 TX measurement (uplink)		1	\$5,760	\$5,760
• CMW-KS500: LTE FDD SISO signaling/network emulation		1	\$8,862	\$8,862
• Installation Accounting Codes		1	\$1,125	\$1,125
• Calibration Accounting Codes		1	\$2,030	\$2,030
Amarisoft LTE 100 eNB Software License	Amarisoft, www.amarisoft.com	1	\$4,947	\$4,947
Amarisoft LTE 100 eNB Software License	Amarisoft, www.amarisoft.com	1	\$5,748	\$5,748
Amarisoft LTE 100-64 UE Software License	Amarisoft, www.amarisoft.com	1	\$7,228	\$7,228
Dell Precision Tower 7810 (PC 5)	Dell, Inc. www.dell.com	1	\$6,893	\$6,893
Dell Precision M4800 (Mobile Workstation 2-6)	Dell, Inc. www.dell.com	5	\$2,148	\$10,740
Dell Precision Tower 5810 (PC 1-3)	Dell, Inc. www.dell.com	3	\$2,735	\$8,206
Dell Mobile Workstation M4800 (Mobile Workstation 1)	Dell, Inc. www.dell.com	1	\$2,367	\$2,367
Dell Mobile Workstation: Mobile Precision 7510 (Mobile Workstation 7-8)	Dell, Inc. www.dell.com	2	\$2,144	\$4,288
Dell Precision Rack 7910: Rackmount Workstation	Dell, Inc. www.dell.com	1	\$10,618	\$10,618
Ettus Research Octoclock	National Instruments, www.ni.com	1	\$909	\$909
Ettus Research USRP N210 w/ SBX daughterboards	National Instruments, www.ni.com	3	\$2,197	\$6,591
Ettus Research USRP B210	National Instruments, www.ni.com	2	\$1,100	\$2,200
Ettus Research USRP B210 w/ enclosures	National Instruments, www.ni.com	8	\$1,194	\$1,958
Ettus Research USRP B210 w/ enclosures	National Instruments, www.ni.com		\$1,194	\$7,594
Ettus Research USRP E310 Kit	National Instruments, www.ni.com	4	\$2,700	\$10,800
RF Switch: RC-2SP4T-A18 + BKT-272-08+	MiniCircuits, www.minicircuits.com	4	\$2,210	\$8,840
RF Switch: RC-8SPDT-A18 + BKT-272-08+	MiniCircuits, www.minicircuits.com	1	\$2,625	\$2,625
Antenna Switch: RC-8SPDT0A18	MiniCircuits, www.minicircuits.com	2	\$2,595	\$5,190
NEMA4 Aluminum Enclosure with Panel	State Electric Supply Company	1	\$468	\$468

⁷ Including discounts, where available

Table M.2. Auxiliary equipment. The shaded rows indicate products that were obtained under ARO/DURIP grant # W911NF-14-1-0553.

Product	Source	#	Unit Price ⁸	Total Price
Intel NUC-i5 Mini PC (w/o RAM and SSD)	B&H	1	\$343	\$343
• Kingston 8 GB RAM	Technology Integration Group	2	\$30	\$60
• Samsung 850 Evo 250 GB M.2 SSD	Dell Marketing LP	1	\$86	\$86
Intel NUC-i7 Mini PC (w/o RAM and SSD)	CDW-G	2	\$584	\$584
• Crucial 32 GB RAM	B&H	2	\$114	\$228
• Samsung 950 Pro 256 GB M.2 SSD	B&H	2	\$190	\$380
Huawei B593s-22 4G LTE UE	Ebay, www.ebay.com	1	\$215	\$215
Huawei E8278s-602 4G LTE UE	Ebay, www.ebay.com	1	\$199	\$199
Sierra Wireless NETGEAR Aircard 330U	Amazon, www.amazon.com	1	\$95	\$95
LTE/WiFi user equipment: Huawei	Ebay, www.ebay.com	1	\$423	\$423
LTE test SIM cards (CMW-Z04)	Rohde & Schwarz	2	\$135	\$270
LTE test SIM cards (CMW-Z04)	Rohde & Schwarz	7	\$135	\$945
Samsung 250 GB T3 Portable SSD	Amazon	5	\$104	\$520
Monitors with stand	Dell, Inc. www.dell.com	2	\$250	\$500
RF and Network Cables and Accessories	Various			\$4,430
RF and Network Cables and Accessories	Various			\$3,111
Indoor Omni Thru Ceiling Mount Antenna	Tessco Inc.	5	\$83	\$414
Directional Coupler: ZHDC-10-63-S+	MiniCircuits, www.minicircuits.com	3	\$85	\$255
Fixed Attenuators: BW-S10W2+	MiniCircuits, www.minicircuits.com	5	\$30	\$150
Fixed Attenuators: BW-S20W2+	MiniCircuits, www.minicircuits.com	6	\$30	\$180
USB DVI KVM Switch	logear	1	\$140	\$140
Multimode Fiber Media Converter Gigabit 10/100/1000 RJ45 (for shielding)	Tripp Lite	2	\$151	\$302
Multimode 62.5/125 Duplex Fiber Patch Cable LC (for shielding)	StarTech.com	2	\$10	\$20
Single-Phase Metered PDU + Isobar Surge Suppression	Trill Lite	1	\$122	\$122
Rack Shelf	StarTech.com	2	\$31	\$62
Mounting Screws and Cage Nuts (100x)	StarTech.com	1	\$64	\$64

⁸ Including discounts, where available

Product	Source	#	Unit Price ⁹	Total Price
USB Switch with Ethernet support		2	\$895	\$1,790
Set of 2 brackets	MiniCircuits, www.minicircuits.com	4	\$30	\$120
Adapter for CMW500 for 19" rack	Rohde & Schwarz	1	\$195	\$195
4-way resistive broadband combiner	MiniCircuits, www.minicircuits.com	1	\$520	\$520
Programmable RF Attenuator: MiniCircuits RCDAT-6000-90	MiniCircuits, www.minicircuits.com	7	\$795	\$5,565
RF Combiners: ZHDC-10-63	MiniCircuits, www.minicircuits.com	1	\$252	\$252
Netgear ProSAFE Gigabit Smart Switch	Netgear	1	\$213	\$213
Broadband SMA power divider/combiner	JFW Industries Inc	1	\$520	\$520
Male mannequin	Store Supply Warehouse	1	\$139	\$139
Samsung 1TB 840 Evo-Series SATA III Internal SSD (hard drive)	Newegg.com	1	\$449	\$449
StarTech.com Mini HDMI to DVI-D Cable	WFCF/DALY Computers Inc.	1	\$9	\$9

⁹ Including discounts, where available

Appendix N

Scholarly Research Contributions

Relevant research has been enabled by the testbed and the initial research results have been published in scholarly articles and presented at conferences of high prestige. The published or to be published papers are listed below; others are still under review.

Journal and Magazine Papers:

- M. Labib, V. Marojevic, J.H. Reed, A.I. Zaghloul, “Enhancing the robustness of LTE systems: analysis and evolution of the cell selection process,” *IEEE Commun. Mag.*, *accepted Aug. 2016, to be published*.
- M. Lichtman, R. Jover, M. Labib, R. Rao, V. Marojevic, J.H. Reed, “LTE/LTE-A jamming, spoofing, and sniffing: threat assessment and mitigation,” *IEEE Commun. Mag.*, April 2016.

Peer Reviewed Conference Papers:

- M. Labib, V. Marojevic, J. Reed, A. Zaghloul, “How to enhance the immunity of LTE systems against RF spoofing,” *Proc. Int. Conf. on Computing, Networking and Communications (ICNC 2016)*, Kauai, Hawaii, 15-18 Feb. 2016.
- M. Labib, V. Marojevic, J. Reed, “Analyzing and enhancing the resilience of LTE/LTE-A,” *Proc. 1st IEEE Conf. Standards for Communications and Networking (CSCN)*, Tokyo, Japan, 28-30 Oct. 2015.